US010855446B2

(12) **United States Patent**
Ow et al.

(10) **Patent No.: US 10,855,446 B2**
(45) **Date of Patent: Dec. 1, 2020**

(54) **AUTONOMOUS EXCHANGE VIA ENTRUSTED LEDGER**

(71) Applicant: **Duvon Corporation**, Las Vegas, NV (US)

(72) Inventors: **Benedict Ow**, Las Vegas, NV (US); **Richard Stiles**, Las Vegas, NV (US); **Anthony Tan**, Las Vegas, NV (US)

(73) Assignee: **Duvon Corporation**, Las Vegas, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 247 days.

(21) Appl. No.: **15/961,521**

(22) Filed: **Apr. 24, 2018**

(65) **Prior Publication Data**

US 2019/0327081 A1 Oct. 24, 2019

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04L 9/06	(2006.01)
G06Q 40/00	(2012.01)
H04L 9/32	(2006.01)
G06F 21/60	(2013.01)
G06F 21/62	(2013.01)

(52) **U.S. Cl.**

CPC ***H04L 9/0637*** (2013.01); ***G06F 21/602*** (2013.01); ***G06F 21/6245*** (2013.01); ***G06Q 40/12*** (2013.12); ***H04L 9/3213*** (2013.01); ***H04L 63/0428*** (2013.01)

(58) **Field of Classification Search**

CPC G06Q 20/065; G06Q 20/3678; G06Q 20/38215; G06Q 40/12; H04L 9/0891; H04L 9/30; H04L 9/32; H04L 9/3239; H04L 9/3247; H04L 9/0637; H04L 9/3213; H04L 63/0428; G06F 21/602; G06F 21/6245

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2018/0025442	A1*	1/2018	Isaacson	G06Q 20/40 705/26.62
2018/0121909	A1*	5/2018	Christidis	H04L 9/3236
2018/0144156	A1*	5/2018	Marin	G06F 21/602
2018/0198624	A1*	7/2018	Bisti	H04L 9/0891
2018/0285983	A1*	10/2018	Franaszek	G06Q 40/12
2018/0337769	A1*	11/2018	Gleichauf	G06Q 20/065
2019/0147438	A1*	5/2019	Micali	H04L 9/3255 705/71
2019/0287107	A1*	9/2019	Gaur	H04L 9/3239
2019/0314726	A1*	10/2019	Masini	A63F 13/71

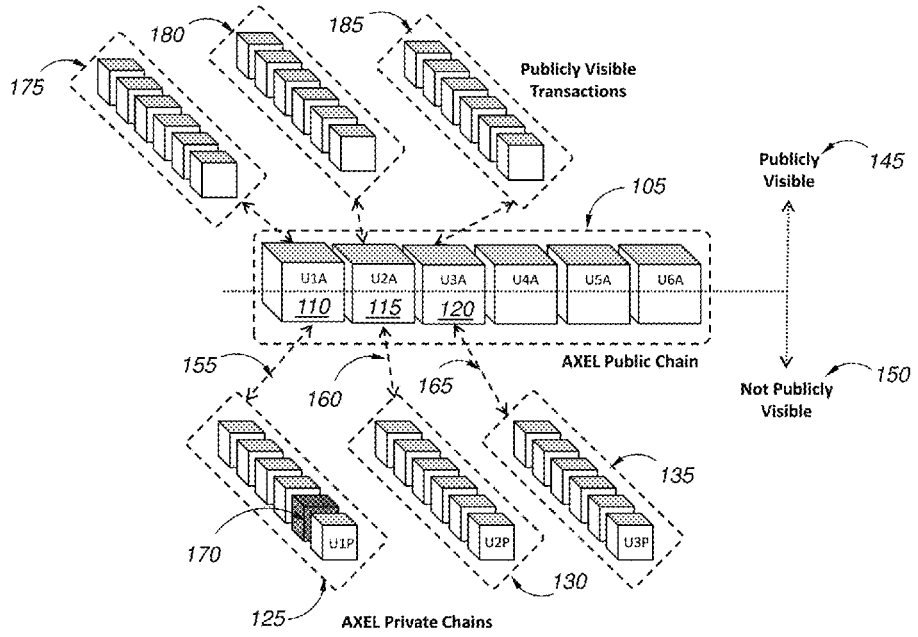
* cited by examiner

Primary Examiner — Malcolm Cribbs
(74) *Attorney, Agent, or Firm* — Lightbulb IP, LLC

(57) **ABSTRACT**

An Autonomous Exchange via Entrusted Ledger (AXEL) blockchain is discussed herein. The AXEL blockchain enables users to perform transactions in a private setting while enabling the transaction records thereof to be verified by other network users without publicly divulging the contents or details of the transaction records.

20 Claims, 8 Drawing Sheets



U7A

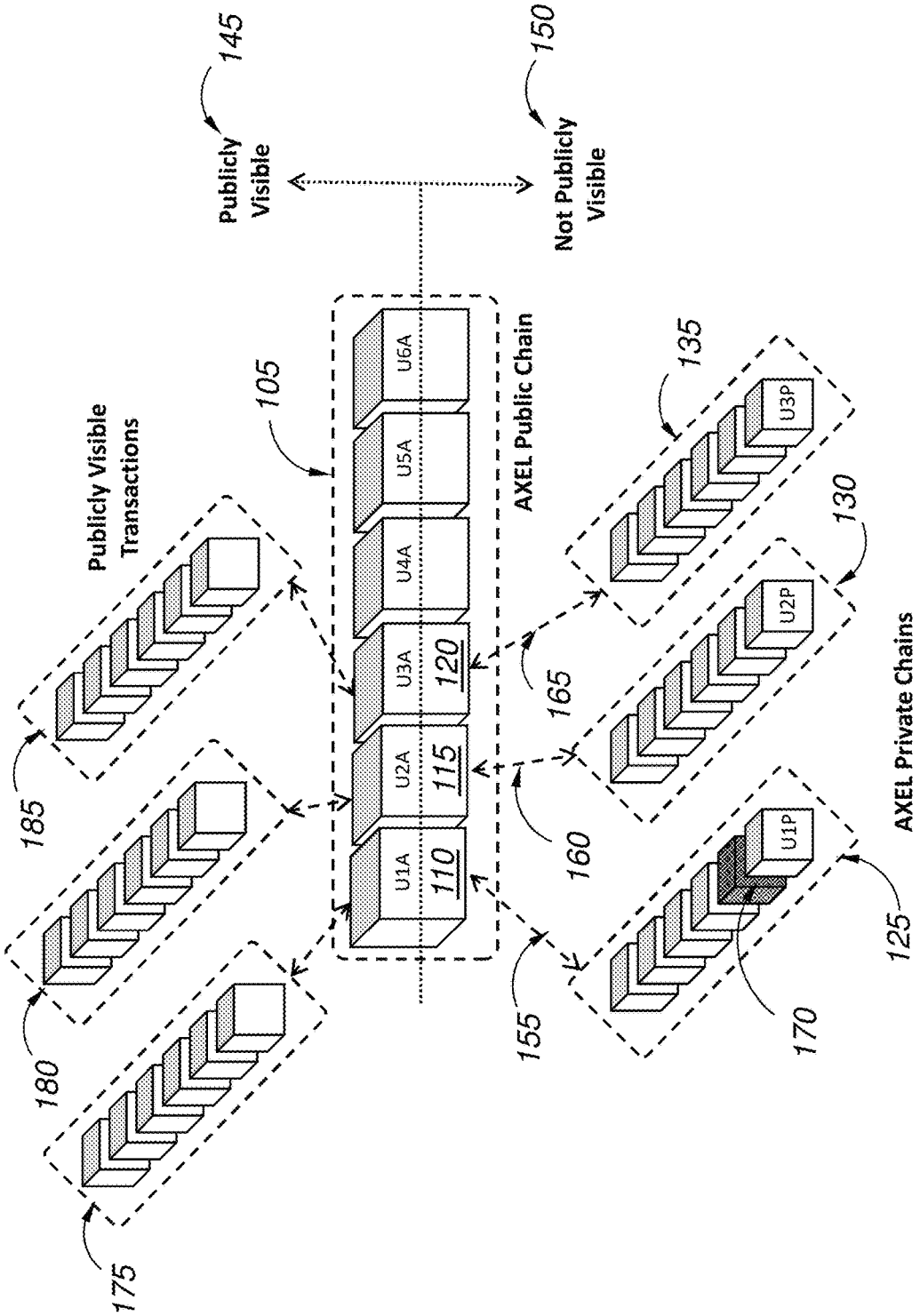

145
Publicly Visible
150
Not Publicly Visible
105
AXEL Public Chain
U1A
U2A
U3A
U4A
U5A
U6A
110
115
120
Publicly Visible Transactions
185
180
175
135
130
125
U1P
U2P
U3P
AXEL Private Chains
155
160
165
170

FIG. 1

U7A

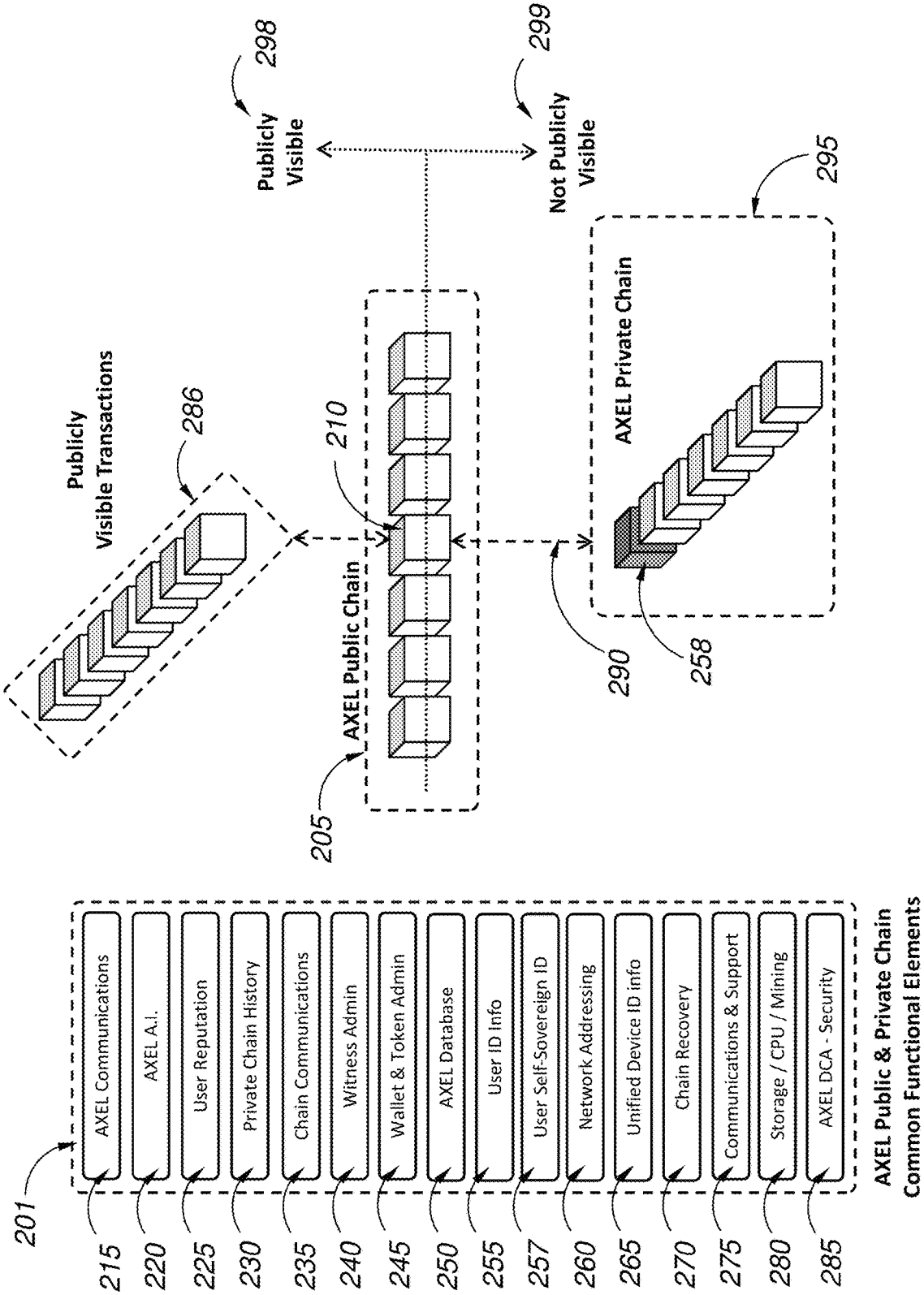

298
Publicly Visible
299
Not Publicly Visible
295
Publicly Visible Transactions
286
210
AXEL Public Chain
AXEL Private Chain
290
258
205
201
AXEL Communications
AXEL A.I.
User Reputation
Private Chain History
Chain Communications
Witness Admin
Wallet & Token Admin
AXEL Database
User ID Info
User Self-Sovereign ID
Network Addressing
Unified Device ID info
Chain Recovery
Communications & Support
Storage / CPU / Mining
AXEL DCA - Security
215
220
225
230
235
240
245
250
255
257
260
265
270
275
280
285
AXEL Public & Private Chain Common Functional Elements

FIG. 2

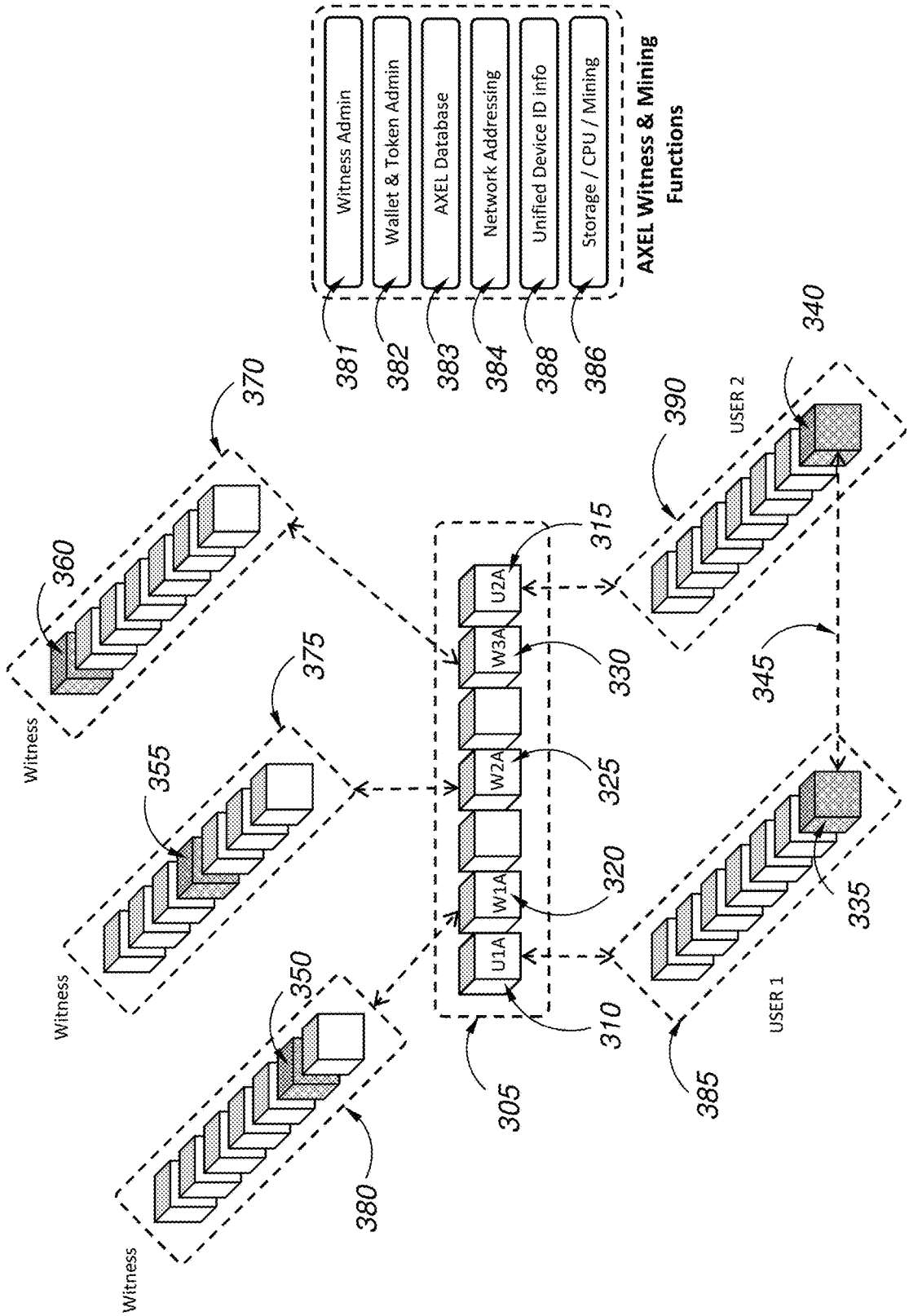

Witness Admin
Wallet & Token Admin
AXEL Database
Network Addressing
Unified Device ID info
Storage / CPU / Mining
AXEL Witness & Mining Functions
381
382
383
384
388
386
370
360
Witness
375
355
Witness
350
Witness
380
305
U1A
W1A
W2A
W3A
U2A
310
320
325
330
315
USER 1
USER 2
385
335
345
390
340

FIG. 3

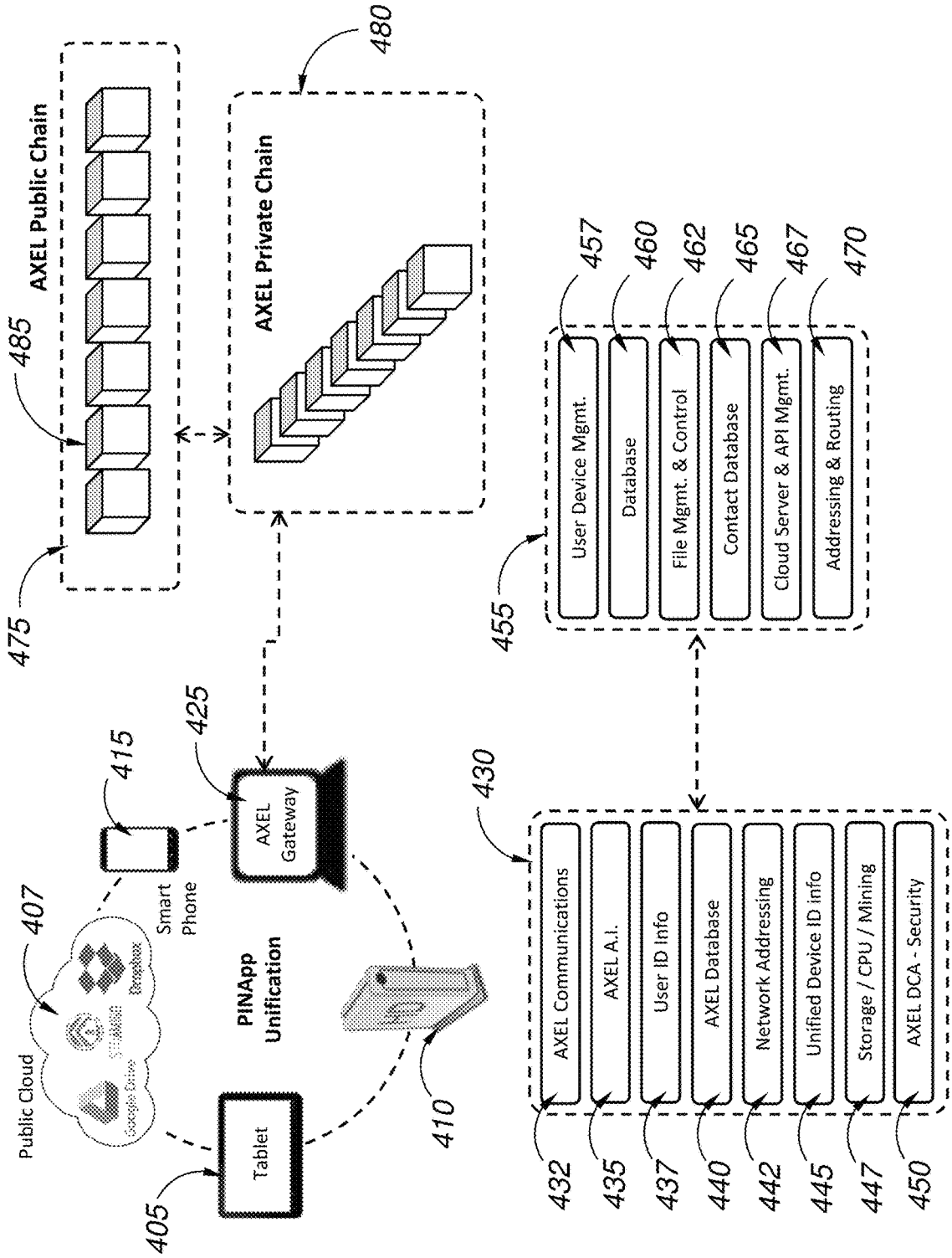

AXEL Public Chain
AXEL Private Chain
485
475
480
User Device Mgmt.
Database
File Mgmt. & Control
Contact Database
Cloud Server & API Mgmt.
Addressing & Routing
457
460
462
465
467
470
455
415
425
AXEL Gateway
Smart Phone
407
Public Cloud
PINApp Unification
Tablet
405
410
430
AXEL Communications
AXEL A.I.
User ID Info
AXEL Database
Network Addressing
Unified Device ID info
Storage / CPU / Mining
AXEL DCA - Security
432
435
437
440
442
445
447
450

FIG. 4

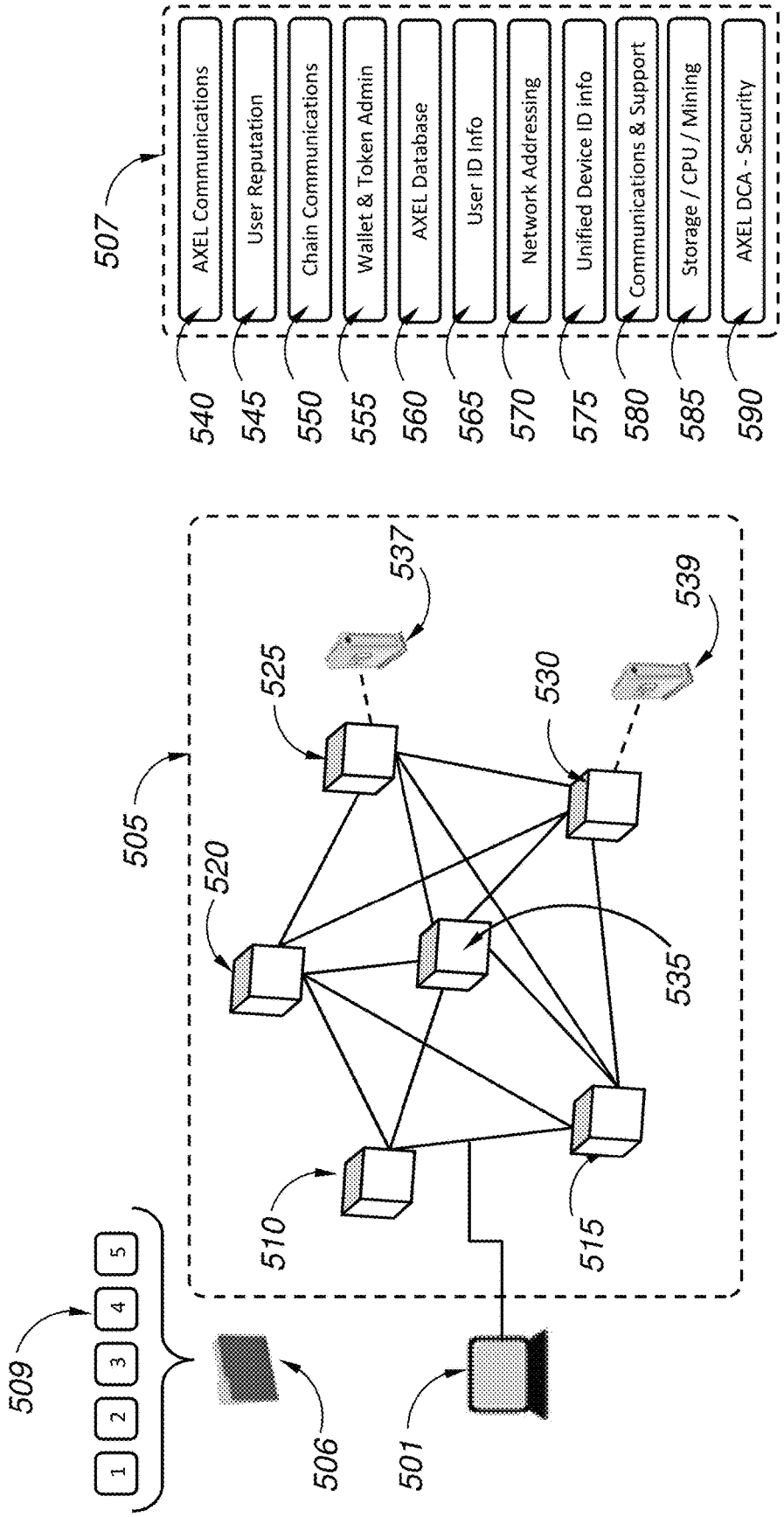

507
AXEL Communications
User Reputation
Chain Communications
Wallet & Token Admin
AXEL Database
User ID Info
Network Addressing
Unified Device ID info
Communications & Support
Storage / CPU / Mining
AXEL DCA - Security
540
545
550
555
560
565
570
575
580
585
590
505
509
1
2
3
4
5
506
501
510
515
520
525
530
535
537
539

FIG. 5

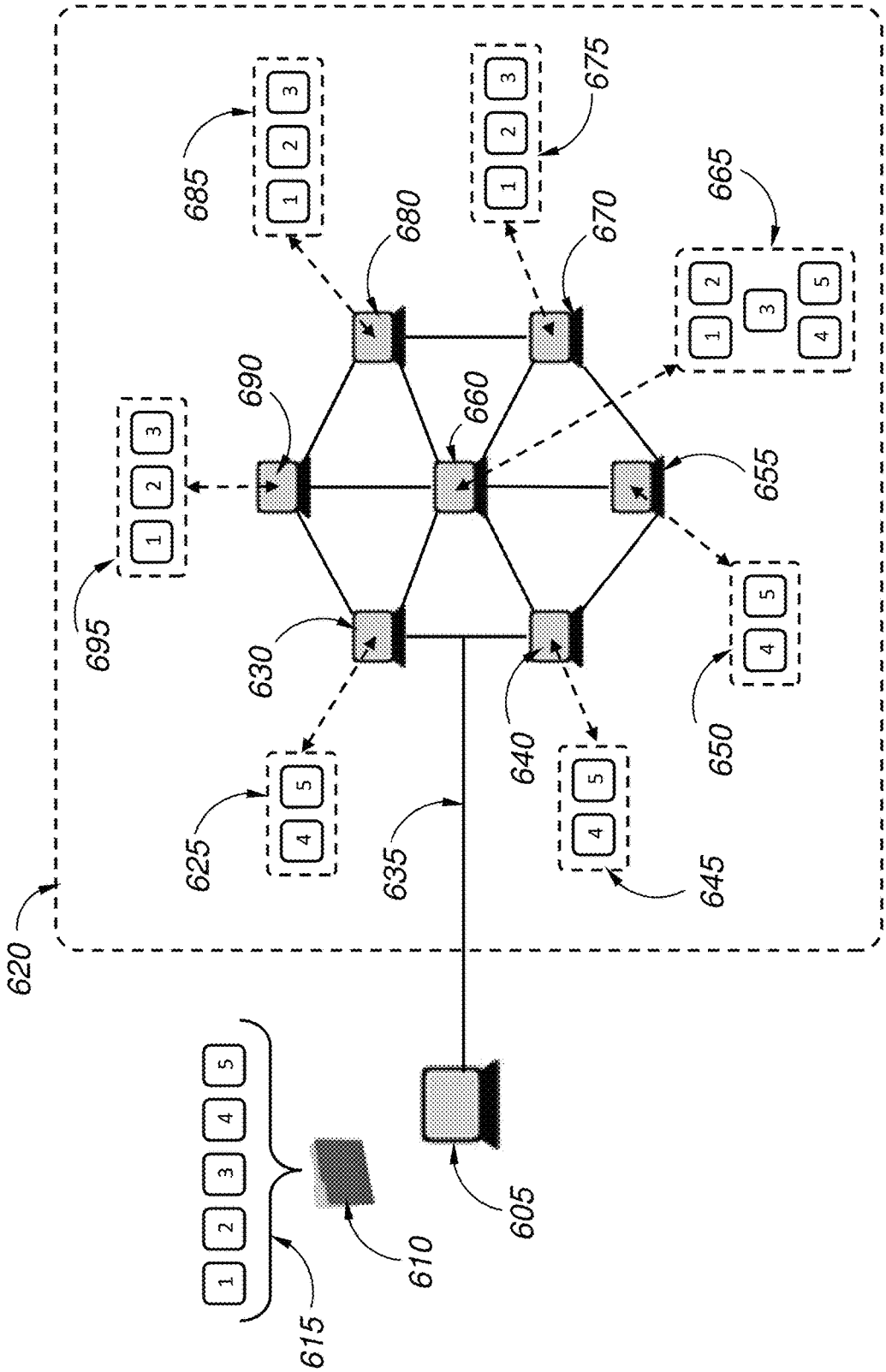

620
615
610
605
635
625
630
640
645
650
655
660
665
670
675
680
685
690
695
1
2
3
4
5

FIG. 6

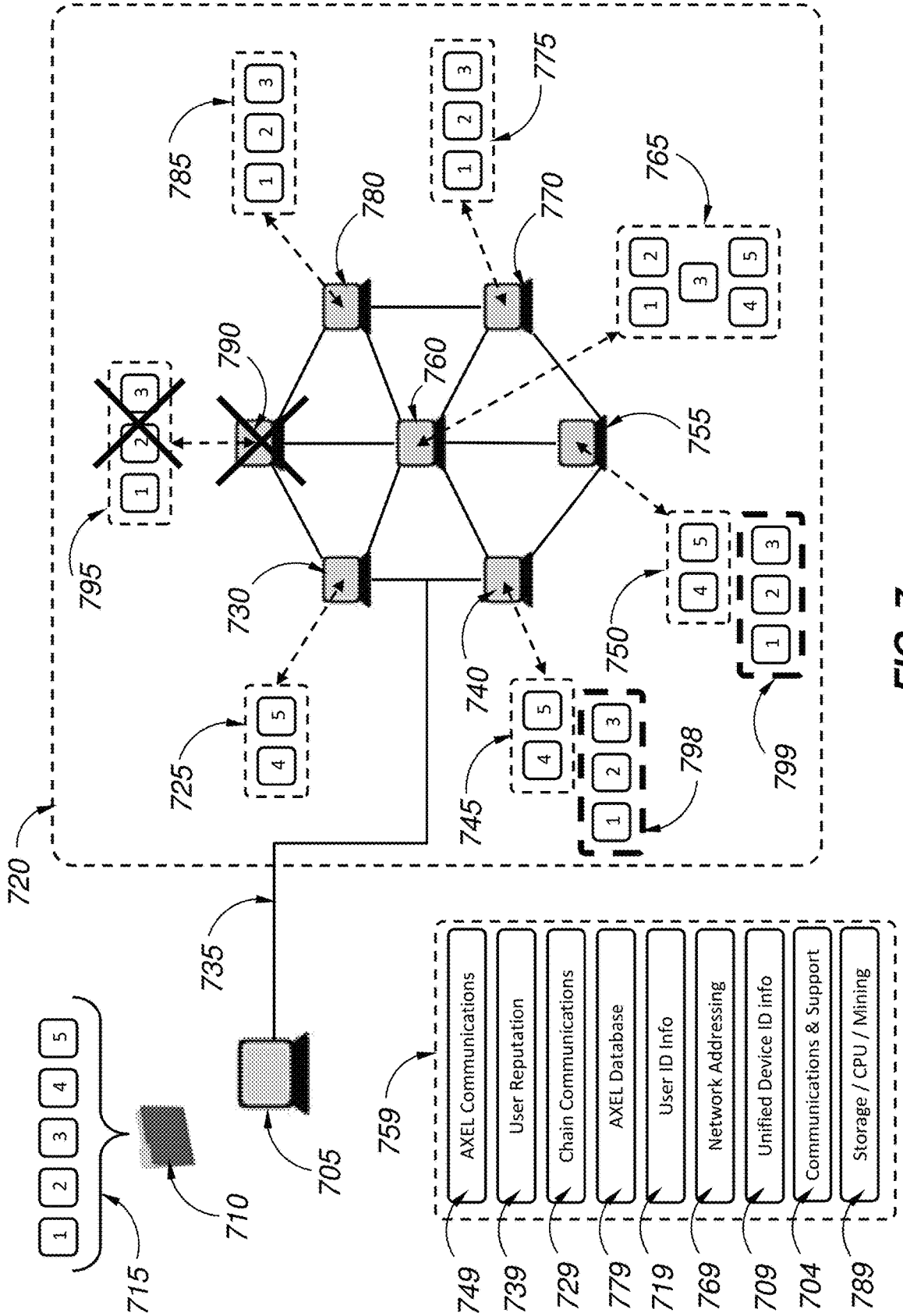
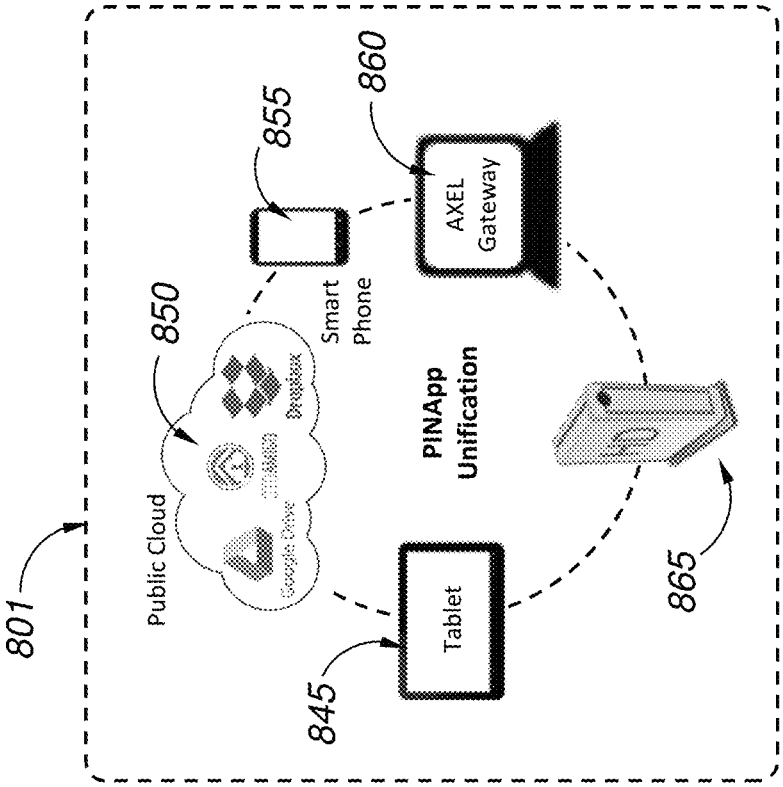

720
735
705
710
715
759
AXEL Communications
User Reputation
Chain Communications
AXEL Database
User ID Info
Network Addressing
Unified Device ID info
Communications & Support
Storage / CPU / Mining
749
739
729
779
719
769
709
704
789
785
780
775
770
765
790
760
755
795
730
750
740
725
745
798
799

FIG. 7


801
Public Cloud
850
855
Smart Phone
860
AXEL Gateway
PINApp Unification
Tablet
845
865

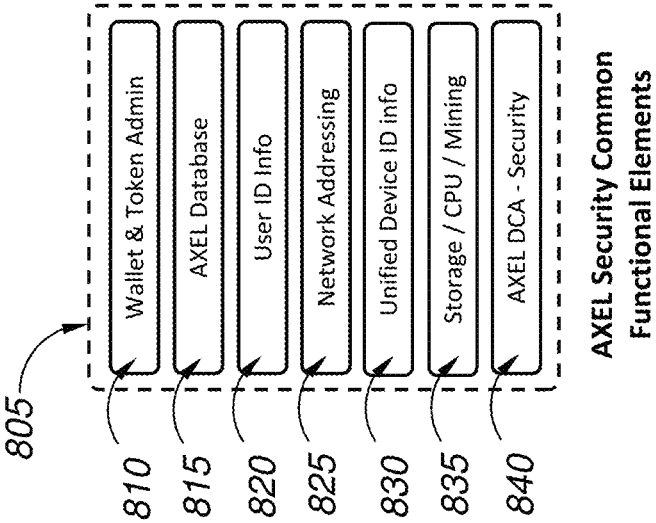

805
Wallet & Token Admin
AXEL Database
User ID Info
Network Addressing
Unified Device ID info
Storage / CPU / Mining
AXEL DCA - Security
810
815
820
825
830
835
840
AXEL Security Common Functional Elements

FIG. 8

AUTONOMOUS EXCHANGE VIA ENTRUSTED LEDGER

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to blockchain architecture that provides both public and private chains (ledger mechanisms) to enable transactional tracking and reporting in a publicly visible environment, while enabling privacy protection to ensure a level of privacy of transaction records.

2. Related Art

Blockchain or distributed ledger technology provides a decentralized architecture for validation of records. Traditionally, the blockchain or distributed ledger and the information therein is shared across participating network nodes.

From the discussion that follows, it will become apparent that the present invention addresses the deficiencies associated with the prior art while providing additional advantages and benefits not contemplated or possible with prior art constructions.

SUMMARY OF THE INVENTION

An Autonomous eXchange via Entrusted Ledger blockchain (hereinafter "AXEL") is described herein. AXEL is a distributed blockchain network that utilizes a suite of unique smart contracts to facilitate the transfer, storage, sharing, and streaming of digital content through the network enabling trust to be established between nodes while providing private transaction capabilities for participants within the AXEL blockchain. While the following disclosure provides an example of the AXEL blockchain in a decentralized network configuration, the AXEL blockchain can easily be configured to support centralized architectures in both public, private, and hybrid deployment configurations.

AXEL is intended to provide a networking environment wherein transactions that occur between parties can be done in a private setting while still enabling the network trust element of a publicly available ledger. AXEL utilizes a unique public and private chain (ledger) approach to decentralized computing wherein the details of transactions that occur between parties remain hidden from public view. In one preferred embodiment, a file can be transferred between a first and a second user. The transaction record of the file transfer will appear in detail on the private ledger of both the first and the second user. Witnesses to this transaction can execute the consensus algorithm to ensure that the transaction has occurred and has been verified, but the user hosting a node that is a witness will not know or have visibility to the details of the actual transaction. This enables the first and second user to maintain the privacy of their transaction while still enabling the blockchain to witness and verify the transaction to ensure authentication and accuracy.

AXEL provides participants with the capability of managing digital content in a blockchain environment. In this example, the storage, transfer, sharing, and streaming capabilities are controlled directly by the user and not through a centralized control mechanism.

The AXEL blockchain may include a utility token mechanism that enables users to create a commerce capability wherein they may trade access or download rights to digital content they own and manage within AXEL in exchange for utility tokens.

In one embodiment, the AXEL blockchain enables a user of a computing device (e.g. personal computer, smartphone, tablet, etc.) to access and manage any digital content located on the subject device (either from that same device or through another device) and provide access to the content through the AXEL blockchain. This embodiment may, in one advantageous configuration, work in conjunction with the PINApp (Pervasive Intermediate Network Attached Storage Application) platform, which is described in U.S. Pat. No. 9,792,452 to enable access and management of digital content.

As one example of the use of AXEL, an AXEL user such as a healthcare provider may wish to transfer patient records privately and securely through AXEL to a health insurance provider. The healthcare provider may select the patient records they wish to transfer and initiate the exchange to the insurance provider. The insurance provider would receive the subject patient records and acknowledge receipt through AXEL.

The transaction in the scenario above is witnessed by a randomly selected group of nodes running a witness consensus algorithm against the subject transaction. Using a consensus algorithm, witnesses reach a consensus and resolve the transaction. As the consensus is completed, the healthcare providers' private blockchain (ledger) will be updated with a block showing the transaction that occurred with the insurance provider. In a similar fashion, the insurance providers' private blockchain (ledger) would also be updated with a block that mirrored the block created for the healthcare provider. These mirror blocks would appear on the subject blockchains (ledgers) of each party participating in a transaction. The witness parties' private blockchains (ledgers) would also contain a mirror block reflecting the transaction that they witnessed.

At the conclusion of the subject transaction in the example above, each participating party (healthcare provider, insurance provider, and witnesses) would automatically update their private blockchains (ledgers) to their alpha blocks associated with each user. The updates to the alpha blocks would contain a verification that the transaction was witnessed and that it was successfully authenticated and verified, validating the subject transaction. In the interest of privacy, the updates to the alpha blocks associated with the transaction would not contain any details of the transaction that took place that are visible to users outside of the immediate transaction other than the transaction was witnessed, authenticated, and verified.

The details of the transaction in the above sequence will be available and visible only to the parties that were directly involved in the transaction (in this example, the healthcare provider and insurance provider). Since the transaction is of a private nature, the transaction details will not be made available to parties outside of the immediate transaction.

The devices used by the witness pool executing the consensus algorithm against the transaction will have access to the details of the subject transaction during the consensus process, but these details will not be visible to the user(s) whose devices are executing the consensus algorithm. These details will be hidden from view to maintain the privacy of the transaction. Once the transaction is completed and digitally signed by the witness pool, each witness will have a mirror block of the subject transaction added to their private ledger (chain). The mirror blocks created for the witnesses will contain, but will not enable visibility to, the details of the subject transaction. The mirror blocks are a key component of the AXEL blockchain as they provide a safeguard against parties who may try to alter or otherwise

compromise the conditions or details of a transaction. By making the transaction details invisible to users outside of the immediate transaction, the AXEL network can protect the integrity of the transactions that occur within the AXEL blockchain while still providing an accurate account of the transaction verification on the public blockchain.

In order to assist with providing adequate storage to facilitate a desirable environment for transactions, the AXEL blockchain can include a distributed network storage capability that allows nodes participating in AXEL to sell storage space that is attached to their local area network devices. In one preferred embodiment, a user may create a node with a personal or home computing device such as a personal computer. The user may attach a one terabyte external storage drive to that personal computer and make the space on that storage drive available for use by other participants within the network.

Unlike existing distributed and decentralized storage methods, in a preferred embodiment, AXEL stores the key codes for both encryption and decryption of the content destined for the network storage on their gateway device such as a personal computer. This ensures the privacy and security of the content being stored as the keys required to access and execute the stored content resides with the user who owns the content.

AXEL can also utilize a redundant storage algorithm that distributes the encrypted parts of the digital content being stored and places them on multiple (participating) devices throughout the AXEL blockchain. In this embodiment, AXEL may routinely request ID and storage information from the network to ensure that the content being stored is both available and accessible to the user. Should a node go offline rendering the stored content unavailable, AXEL may notify the gateway device that the content is no longer available and create additional backup copies of the content that is no longer available. These copies could be gathered from other repositories within the network storing identical encrypted fragments of the subject digital content throughout the AXEL blockchain.

AXEL can also incorporate mechanisms to comply with identification and anti-corruption due diligence requirements, such as regulations directed at money laundering activities. For example, to comply with current regulations AXEL may include an "anti-money laundering" (AML) and "know your customer" (KYC) mechanism to ensure positive identity of the participants on the AXEL blockchain. At account creation, users will disclose information about themselves during the sign up process, as well as information about the devices they are utilizing to connect to the AXEL blockchain.

If PINApp is used with AXEL, device information can be collected through the PINApp and stored in the users' private chain. Information about the device such as the MAC code will be kept in the users' private ledger (chain) to ensure that if someone were to steal their login and access information, they would be unable to access the AXEL network because the device they are utilizing is not registered to the network. In a like fashion, a person using a registered device may not access the AXEL network without the proper login and authentication information.

The AXEL blockchain can utilize functional components of the PINApp, and it may also include functional components of the Digital Certification Analyzer ("DCA")—as set forth in U.S. Pat. Nos. 9,419,965; 9,565,184; and 9,723,090—to prevent unauthorized access of digital content. For example, the PINApp could be utilized to perform device unification capabilities allowing AXEL participants to access the AXEL blockchain from remote devices such as smartphones, tablets, and the like. The DCA functional components could be utilized in support of the AML/KYC implementation as well as the multi-factor authentication mechanisms.

In addition to the AML/KYC mechanism disclosed previously, the AXEL blockchain can also incorporate a self-sovereign identity capability that gives users complete control of their identity as well as the capability to privately store and secure the identity content, including any third-party verification and authorization validating the identity. This self-sovereign identity may be deleted, in whole or in part, by the user/owner of the identity in compliance with emerging privacy laws.

The devices, features, and functions described herein are intended to disclose a method to provide readily scalable blockchain architecture that supports the transfer of digital content and other assets, while enabling privacy and security mechanisms to protect the privacy of users, while also providing accuracy of ledger reporting to ensure trust and accountability within the blockchain. Unlike existing blockchain networks, the Autonomous eXchange via Entrusted Ledger (AXEL) network will utilize a unique ledger capability that separates out the public ledger (or public chain) from the private ledger (or private chain) allowing users to conduct transactions privately while still enabling the ledger to be authenticated by a consensus-type algorithm to ensure accuracy and blockchain integrity.

The AXEL blockchain described herein addresses the need for an efficient, scalable, and cost-effective method to allow users to manage transactions relating to digital content and other digital assets through a decentralized network wherein participants can establish a level of trust through the use of a public ledger that will track and record the transactions made within the network. The AXEL blockchain can include a utility-type token mechanism to enable parties to conduct transactions within the network and exchange the tokens in lieu of traditional currencies such as USD and the like.

The AXEL blockchain creates an environment wherein transactions made between one or more parties can be done privately without the need to notify each node in the network that a transaction has occurred, but to additionally enable the ledger to maintain accuracy and track the transactions without divulging the specific details of the transactions that occurred.

The AXEL blockchain additionally can enable the transfer, storage, sharing, and streaming of digital content (e.g. files, folders, movies, songs, etc.) to be presented and available for transactions through the AXEL blockchain. To perform this functionality, the AXEL blockchain may incorporate functional components of the PINApp.

Functionally, PINApp unifies the storage repositories across all users' computing devices and makes the content available to multiple devices as it if were hosted locally in a single repository. By enabling PINApp capability with the AXEL blockchain, users can participate in the storing, sharing, streaming, and transfer of digital content and other digital assets without the requirement to physically upload and/or move any of their content to a specific storage or device in order to allow blockchain access and engagement with the digital content.

In one preferred embodiment, a user of the AXEL blockchain will execute the blockchain gateway on a home computer but be able to access and engage the transactional capabilities of the AXEL blockchain from any of their portable devices. This capability allows a user to participate

in the network from anywhere, negating the need for them to operate the blockchain gateway on each of their devices in order to gain access to the network.

In one preferred embodiment, a first user may wish to sell a digital asset such as a photo that is hosted on a portable device such as a smartphone. The first user may execute the sale transaction directly from the smartphone and engage the AXEL blockchain remotely, negating the need for the first user to physically move or copy the photo to the device running the blockchain gateway.

As the transaction above is executed, a second user (buyer) would execute a purchase through the AXEL blockchain utilizing the utility token and acquire the photo directly from the first user's smartphone hosting the referenced content. This would also negate the need to copy or otherwise move the content to a public cloud or other holding repository to allow the second user (buyer) to gain access.

The transactions occurring (as in the above example) within the AXEL blockchain are recorded to a ledger, enabling the AXEL blockchain to accurately track transactions that occur. Unlike traditional ledger technologies, the AXEL blockchain will utilize a unique ledger methodology that incorporates a public and private component of the ledger.

The public ledger (or chain) will be created in support of the network's need to provide visibility and tracking of the transactions that occur within the blockchain. The private ledger (or chain) will be created on a per-user basis, allowing each user to conduct transactions within the AXEL blockchain and enjoy a level of privacy for their associated transactions. While specific examples are provided herein of specific information that is included on the public ledger or the private ledger, AXEL may be specifically configured to adjust the particular information that is included on the public or private ledger. For example, depending on what types of transactions are contemplated or changes in laws, it may be advantageous or necessary to include more information on the private ledger as compared to the public ledger or vice versa. As another example, it may prove necessary for more information to be included on the public ledger to promote certainty in transaction verification or to better ensure that the system cannot be compromised. Thus, the disclosure herein should not be read as limiting and is only an example of the types of information that may be included on the public and private ledgers.

Each participant within the AXEL blockchain will be assigned an alpha-type block within the public ledger (chain) and a private ledger (chain).

In a preferred embodiment, the private ledger will report to the public ledger alpha block associated with the user. Any transactions that occur within the AXEL blockchain will be recorded immediately to the private ledger of the parties associated with the subject transaction. As the transactions are completed and the private ledger is updated, the updated information is reported from the private ledger to the public ledger alpha block.

The separation of the public chain and the private chain exists to (a) allow the user to enjoy a level of privacy while engaging in their transactions; (b) keep an accurate and ongoing record of each transaction the user is involved in; (c) enable the user to participate in the witness mechanism (described in detail later in this submission) and; (d) to enable the artificial intelligence mechanism (described in detail later in this submission) within the AXEL blockchain to parse the transactional data on behalf of the user and provide guidance and recommendations as to how the user can get more benefit from their participation within the AXEL blockchain.

As transactions are recorded to the AXEL blockchain, the consensus algorithm will incorporate a witness mechanism that is described in detail later in this submission. In one preferred embodiment, the witness mechanism will select a group of nodes (5 to 20 nodes as an example) using a randomized algorithm. The selected group of nodes will perform the consensus calculation against a transaction. Once consensus has been reached by the selected witness group (nodes), the transaction will be digitally signed by the witness(es) and the private ledger (chain) will be updated with a new block (or blocks) reflecting the transaction being recorded. Non-private information pertaining to the subject transaction such as (but not limited to) the authentication of the transaction and the witness nodes participating in the transaction will be visible on the public ledger (chain) in association with the alpha block hosting the private chain where the transaction took place. The incorporation of the witness mechanism allows multiple transactions to occur and be confirmed through the consensus algorithm process simultaneously, speeding up the network transaction capability.

The AXEL blockchain will also provide a user-focused artificial intelligence (AI) component that will collect and parse transactional data on behalf of the user to give them instant access to information that was transacted utilizing the AXEL blockchain. Transactional information such as automobile maintenance schedules, medical history records, prescription drug records, and other lifestyle events can be processed and tracked through the AI functions of the AXEL blockchain.

In one preferred embodiment, the AXEL blockchain AI component will collect and parse information pertaining to the history of a specific user to enable the user to instantly access information including but not limited to medical records, prescription medication history, car maintenance history, general sale and purchase history and other lifestyle metrics that can be managed and tracked through the private ledger and parsed with the artificial intelligence module. The information will be provided to the user based on a query submitted by the user pertaining to their transactional history within the AXEL blockchain.

The purpose of the AI and the data parsing is to further enable the users of the AXEL blockchain to accurately track transactional history and provide feedback and historical information directly to the users of the AXEL blockchain. The AXEL blockchain AI component will act as a personal assistant or personal transaction manager for the user to enable them to easily recall historical information pertaining to transactions within the AXEL blockchain. In a preferred embodiment, the AI component is not intended or designated for use by any company or other entity seeking to collect user information for marketing or other purposes. The information may be stored and parsed at a local level to ensure the security and privacy of the AI functionality.

As previously stated, the user private chain will be updated as each transaction is executed and subsequently verified within the system utilizing a consensus algorithm. In a similar fashion, the user private chain will be updated with a block reflecting the user participation in the witness mechanism. Blocks created on the user (witness) private chain during the nodes' participation in a witness function/event are designated as mirror blocks. These blocks mirror the transaction that the subject node witnessed to ensure the

accuracy of the consensus and to prevent attempts to alter the transaction or the associated blocks hosted within the ledger(s).

The mirror-blocks include details of the transaction that took place during the transaction being witnessed, along with the consensus verification to ensure the block has been verified and/or vetted through the consensus algorithm within the AXEL blockchain. The purpose of the mirror-block is to prevent a party (user) from making a change or augmenting a transaction that has already occurred and been verified within the AXEL blockchain. The witness mechanism and the mirror-block function are described in detail later in this submission.

In one preferred embodiment, the witness mechanism will select a group of nodes (5 to 20 nodes as an example) from the AXEL blockchain using a randomized algorithm. The selected group of nodes will perform the consensus calculation against a transaction. Once consensus has been reached by the selected witness group (nodes), the witness(es) will digitally sign the transaction and the ledger (chain) will be updated with a new block (or blocks) reflecting the transaction being recorded. Each node (witness) participating in the consensus of the subject transaction will create a mirror-block on their own private chain to reflect the transaction in which they participated. The incorporation of the witness-consensus feature allows multiple transactions to occur and be confirmed simultaneously, speeding up the network transaction resolution capability.

In a preferred embodiment, the witness mirror blocks created on the witness private chain during a witness event contain encrypted information which prevents the user of the witness node from seeing any private or personal details from the subject transaction. Details such as party names, items being bought or sold, the pricing of the subject items, vendor names, and other private details of the transaction are encrypted to protect the privacy of the parties that participated in the subject transaction. However, in order for the witness function to perform properly, this information is shared (in an encrypted format) with each witness performing the consensus algorithm via the witness function. Once the witness event is complete (regardless of whether the transaction was authorized or declined) the blocks added to the witness ledger will be encrypted to protect the privacy of the participants of the subject transaction.

In another preferred embodiment, nodes participating as witnesses in a transaction will create mirror-blocks which are then added to their respective private ledger (chain) to serve as an indication that the transaction has occurred and been verified through the witness mechanism, that they (the participating node) executed the consensus algorithm of the subject transaction, and to ensure that changes may not be made to a ledger entry that has already been verified within the AXEL blockchain.

In this preferred embodiment, mirror-blocks become a component of each user's private ledger (chain) that participates in a witness event. Since the users of the network do not know when a node will be selected as a witness to a transaction, they cannot accurately predict or target these nodes for purposes such as hacking or introducing non-verified ledger information into the AXEL blockchain. The randomized algorithm that selects the nodes to participate in the witness event prevents any visibility of the transaction details to participating nodes, ensuring accuracy and security of the transactions and ledger updates.

In a preferred embodiment, the AXEL blockchain provides a distributed storage capability to enable participants of the network to store the digital content (e.g. files, folders, images, etc.) on participating computing devices connected to the AXEL blockchain. Unlike typical storage models, the AXEL blockchain stores the encryption and decryption information to support the distributed network storage function directly on the user's (content owner) private chain. This prevents visibility to the user encryption data, and subsequently the files and digital content being stored within the network. By locally storing the encryption and decryption information on the user's local private chain, the AXEL blockchain ensures availability of the keys utilized to manage the stored content.

The AXEL blockchain will routinely query the participating storage repositories to ensure the content being stored within the AXEL blockchain continues to remain in the location in which it was stored. Due to the distributed and decentralized nature of the storage repositories that will be connected to the AXEL blockchain, continuous verification of file storage accessibility, integrity, and availability is paramount to ensuring the security of the stored content.

In a preferred embodiment, the digital content stored within the AXEL blockchain will be stored redundantly, ensuring the availability of stored content in cases wherein the device storing the subject content becomes unavailable due to being offline or for other unforeseen circumstances. In one preferred embodiment, a file may be locally fragmented and encrypted on the user device utilizing the distributed decentralized storage capability to store the file within the AXEL blockchain. The subject file fragments will then be sent to participating network storage nodes that will store the encrypted fragments. The participating nodes will host various fragments of the file to ensure redundancy, availability, and accessibility to the file owner within the AXEL blockchain. In one preferred embodiment, the same encrypted fragment portion of a file may be stored in a variety of locations within the AXEL blockchain to ensure redundancy and availability of the subject file. The location of the fragments and the contents therein will be known by no one within the AXEL blockchain except the file owner.

The AXEL blockchain will incorporate a unique user identification block that will contain information required to provide a positive identification of the user and their associated engagement with the AXEL blockchain. The user identification block will be created on the private chain component of the AXEL blockchain and remain in control of the user who owns the physical identification being written digitally to the identification block.

Unlike identifications created by third-parties such as online shopping websites, eCommerce websites and the like, the user identification block will be created by and controlled by the user/owner of the identification. The user/owner may then allow (at their sole discretion) a party to authenticate the identity of the user/owner to facilitate both digital and physical transactions that may occur and/or be recorded through the AXEL blockchain.

In one preferred embodiment, a user may create an identification block that provides a positive identity of the user and meets all legal requirements as such. In this embodiment, the identity will be under the complete control of the user/owner of the identity and may be deleted at any time, completely removing the user/owner identity from the AXEL blockchain. The user/owner of the identification will hold privacy-type keys that control the access to the identity and the usage thereof. A public key may be provided to a third party by the user identification owner to enable that third party to execute a one-time authentication of the identification of the user to enable eCommerce and other

transactions of both physical and digital nature(s) that can be managed through the AXEL blockchain.

The user identity will be stored in a digital vault that is managed solely by the user identity owner. This vault (similar to a digital wallet) will be controlled by keys that the user/owner of the identification can share at their discretion to enable others to positively identify the user/owner for the purpose of transactions requiring such identification. The vault will exist on the user/owner controlled device(s) and may be backed-up to ensure integrity of the identity. As third-parties are allowed to verify the identity of the user/owner, these verification authorizations and confirmations will also be stored in the user identity vault to further add to the validity and authenticity of the user/owner identity.

The user identity block created on the private chain will support a self-sovereign control mechanism ensuring the user identity block can be both completely separated from the AXEL blockchain as well as to be deleted in its entirety. While the deletion of the user identity block will support legal requirements relating to "right to be forgotten" and other identity protection laws, the deletion of the user identity block will not negatively affect the authenticity of the transactions that occurred while the user was a participant in the AXEL blockchain. The user identity block may not be removed by anyone but the user/owner of the user identity block.

Other systems, methods, features and advantages of AXEL will be or will become apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional systems, methods, features and advantages be included within this description, be within the scope of the invention, and be protected by the accompanying claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The components in the figures are not necessarily to scale, emphasis instead being placed upon illustrating certain embodiments of the invention. The drawings are intended to illustrate particular configurations of the AXEL blockchain, but it should be understood that AXEL allows for variation of these configurations. In the figures, like reference numerals designate corresponding parts throughout the different views.

FIG. **1** is a diagram illustrating the public and private chain elements of AXEL;

FIG. **2** is diagram illustrating the functional aspects of the AXEL blockchain;

FIG. **3** is a diagram illustrating the witness function of the AXEL blockchain;

FIG. **4** is a diagram illustrating the PINApp unification and associated functions of the AXEL blockchain;

FIG. **5** is a diagram illustrating the resource assessment algorithm function;

FIG. **6** is a diagram illustrating the distributed storage function within the AXEL blockchain;

FIG. **7** is a diagram illustrating the redundancy of the distributed storage function; and

FIG. **8** is a diagram illustrating the security and user identification functions utilizing the DCA within the AXEL blockchain.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following description, numerous specific details are set forth in order to provide a more thorough description of the present invention. It will be apparent to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known features have not been described in detail so as not to obscure the invention.

As previously stated, AXEL is comprised of two distinct and separate blockchains: a public blockchain that is provided to enable public visibility to transactional history and a private blockchain to allow users within the AXEL blockchain to conduct their transactions privately between consenting parties. Each user within the AXEL network will be assigned both a publicly visible alpha-type block that resides on the public chain, and a private chain in which their personal transactions may be conducted to insure privacy and discretion.

The purpose of the AXEL blockchain's two-chain approach is to allow users to conduct their daily transactions in a more private setting, while at the same time enabling the consensus and verification of the transactions to be shared through a publicly visible ledger represented by the public blockchain.

For the purpose of the discussions that follow a node is a computer or other computing-type terminal that is running at least a portion of the AXEL gateway client software. Nodes communicate with each other through the AXEL gateway client software and create a decentralized distributed network to operate the AXEL blockchain. Storage of the public and private blockchains discussed herein may be facilitated through localized storage at the node location, localized storage at the user location (in reference to private chains). Additionally, storage of the reference chain elements can be managed through the AXEL distributed decentralized network storage capability or any combination thereof.

A general description of the chain mechanisms will now be described with reference to FIG. **1**. As can be seen in FIG. **1**, the AXEL public chain **105** is comprised of blocks (**110**, **115**, **120**, etc.) designated as alpha blocks (U**1**A=User **1** alpha block, U**2**A=User **2** alpha block, etc.). These alpha blocks are created to represent each participant/user that creates an account and participates in the AXEL blockchain. The alpha block (described in detail in the pages that follow) is designated to store the historical data for the user in which the alpha block is designated and represents the publicly visible aspects of the user profile. As can be seen in FIG. **1** the AXEL public chain **105** is comprised of user alpha blocks (U**1**A, U**2**A, etc.). The user **1** alpha block **110** is designated as the publicly visible profile for user **1** and is paired **155** with a private chain **125**. In a similar fashion, the user **2** alpha block **115** is paired **160** with a private chain **130**. User **3** alpha block **120** is also paired **165** with a private chain **135**. Each alpha block (**110**, **115**, and **120**) is designated and assigned to its respective user private chain (**125**, **130**, and **135** respectively).

The pairing indicators (**155**, **160**, and **165** respectively) represented in FIG. **1** are intended to show both the relationship of the respective alpha blocks (**110**, **115**, and **120**) with their private chain counterparts (**125**, **130**, and **135**) but also to demonstrate a direct communication link associated with each alpha block (**110**, **115**, and **120**) to their respective private chains (**125**, **130**, and **135**).

The communications **155**, **160**, and **165** provide direct engagement for each of the private chains **125**, **130**, and **135** with their respective alpha blocks **110**, **115**, and **120** to ensure the public visibility of the vetted transactions as well as enabling the transfer and logging of transactional information between the alpha blocks (**110**, **115**, and **120**) and their respective private chains (**125**, **130**, and **135**).

As previously stated, the AXEL public chain **105** represents the publicly visible **145** aspects of the AXEL blockchain whereas the private chains **125**, **130**, and **135** represent the components of the AXEL blockchain that are not visible to the public **150**. The purpose of the AXEL public chain **105** and the respective private chains **125**, **130**, and **135** is to enable the users to enjoy a level of privacy while engaging in transactions with other users while still giving the AXEL public chain **105** and the subsequent nodes (not pictured) visibility to the fact that each transaction that occurs on the private chains (**125**, **130**, and **135**) has been verified by the AXEL blockchain.

As an example of the chain utilization, user **1** (private chain **125**) engages in a transaction. Once the transaction has been resolved utilizing the consensus algorithm (witness mechanism discussed later in this submission), a new block **170** is added to the private chain **125**. As the private chain **125** has been augmented with the new block **170**, the private chain **125** communicates **155** the addition of the new block **170** to the user **1** alpha block **110** hosted on the AXEL public chain **105**. This process repeats itself each time a user executes a transaction within the AXEL blockchain.

The details of the above subject transaction **170** will be invisible **150** to other users on the AXEL blockchain with the exception of other user(s) participating in the subject transaction. This gives the users of the AXEL blockchain the capability to conduct their transactions with a level of privacy.

It is important to note that while the transactions occur in a private setting within the AXEL blockchain, in the preferred embodiment, they do not occur with anonymity. As previously stated, the advantages of this are that verification and authentication of identity is beneficial in some instances to comply with certain regulations including, for example Anti-Money Laundering and Know Your Customer regulations. While this information would not be publicly available to other participants in the network, they will know that when they conduct transactions with other users, that these users have been authenticated and vetted by AXEL.

With continued reference to FIG. **1**, as the transaction **170** is updated **155** to user **1**'s associated alpha block **110** the transaction verification becomes publicly visible **145**, but the details of the actual transaction itself do not. As an example (and with continued reference to FIG. **1**), user **1** (not shown) executes a transaction. The transaction involved a purchase made from an online retailer (not pictured). The details of that purchase including (but not limited to) the item purchased/sold, the item price, any applicable discounts, buyer/seller name and contact info, any warranty information, etc. will be visible on user **1**'s private chain **125** as represented by the newly created block **170**. As block **170** is shared **155** to user **1**'s respective alpha block **110** it will be stored in the user's transaction history (explained in detail later in this submission). As the user **1** alpha block **110** is updated, the AXEL public chain **105** will enable the nodes (not pictured) to see that the user **1** alpha block **110** has been updated and verified by the AXEL blockchain, but they will not know the details of the transaction. They will however be able to see that the transaction added to the user **1** alpha block **110** has been vetted and verified by the AXEL blockchain.

Again, in the interest of being able to create a private transaction, the details of the transaction will only be visible to the users directly involved with the subject transaction (in this example the buyer and seller). The remainder of the blockchain users (nodes) will see that a transaction has occurred and has been verified by the system (to ensure validity and transparency pertaining to the transaction history) but will not be able to see the details of the actual transaction.

In a similar fashion if a person were to walk into a pharmacy and make a purchase from the pharmacist, other parties present in the pharmacy would have visibility to the person making a transaction with the pharmacist, but would not be privy to the details of the subject transaction. While the AXEL blockchain is capable of supporting transactions of a completely anonymous nature, in a preferred embodiment users are provided a measure of privacy to conduct transactions within an environment wherein the ledger components can enable a measure of trust to exist between nodes over a distributed and decentralized network.

As stated previously, the alpha blocks are created and hosted within the public chain to represent each user within the AXEL network. Each alpha block acts as a repository and control mechanism for each user and their associated private chain.

In the discussion that follows, functionality that exists on both the public chain and the private chain of the AXEL blockchain will be disclosed. In many cases, like or similar functional elements will be present on both the public chain and private chain components of the AXEL blockchain. FIG. **2** has been simplified to ease understanding of the functionality and to limit redundancy within the descriptions. It will be apparent to one skilled in the art that these functional elements can coexist or be implemented (or not implemented) separately as required by the specific implementation of the AXEL blockchainThe functional elements with reference to FIG. **2** are discussed in the following paragraphs.

As can be seen in FIG. **2**, the public and private chains of the AXEL blockchain share a number of common functional elements **201**. These functional elements **201** are AXEL communications **215**, AXEL A.I. **220**, user reputation **225**, private chain history **230**, chain communications **235**, witness administration **240**, wallet and token administration **245**, AXEL database **250**, user ID info **255**, network addressing **260**, unified device ID info **265**, chain recovery **270**, communications and support **275**, storage/CPU/mining **280**, and the AXEL DCA—security **285** function. Each of these functions within the AXEL blockchain has a presence and designated functional implementation on both the AXEL public chain **205** and the AXEL private chain **295**. Each of these functional elements will be described in detail in the pages that follow.

As can be seen in FIG. **2**, the AXEL public chain **205** is comprised of alpha blocks **210**. Each of these alpha blocks **210** represents a user/participant within the AXEL blockchain. Each alpha block **210** is directly affiliated **290** and in direct communications with a private chain **295** that is utilized to record transactional and use history for each user participating within the AXEL blockchain. It is important to note that the AXEL blockchain can support a virtually unlimited number of users and/or participants. The public chain **205** and private chain **295** references provided show a single user configuration to ease understanding of the figure and to allow for focus on the functional aspects and engagement between the public **205** and private **295** chains respectively.

With continued reference to FIG. **2**, the AXEL communications **215** function resides on both the alpha block **210** and within the private chain **295**. The AXEL communications **215** function provides a mechanism wherein users within the AXEL blockchain can conduct communications between parties. Functions such as an instant message, text

or SMS-type message, email messages, and other communications elements are supported by the AXEL communications **215** function. In one embodiment the AXEL blockchain may be utilized as an electronic marketplace wherein participants may buy and sell goods. A first user may engage the AXEL communications **215** function to leave a message within the marketplace for a second user, or to comment on a product or service the second user may provide. In a similar fashion, the first and second user can engage the AXEL communications **215** function to engage in a private chat or private email type session within the blockchain. The AXEL communications **215** function manages communications between parties utilizing the AXEL blockchain.

The AXEL communications **215** function may utilize the DCA (Digital Certification Analyzer) to enable a first user to send a private message to a second user, and require the second user to initiate the DCA protocol to access the message. The message may also be protected and/or encrypted utilizing the AXEL DCA—Security **285** capability discussed later in this submission.

Communications within the AXEL blockchain can originate from either the public chain **205** or the private chain **295**, depending on the nature of the communications and the needs of the user. As an example, a public message such as a posting to comment on a product purchased from an eCommerce site or other social-type publicly visible message may originate from the alpha block **210** on the AXEL public chain **205**. A private message intended for a specific recipient or group of recipients may originate from the private chain **295**.

The AXEL communications **215** function works in conjunction with the AXEL database **250**, the network addressing **260**, and the AXEL DCA—Security **285** functions to ensure proper configuration and delivery of various message types within the AXEL blockchain.

The AXEL A.I. (artificial intelligence) **220** function is integrated into the AXEL blockchain to support both public chain **205** and private chain **295** capabilities. On the private chain **295** the AXEL A.I **220** function is controlled and managed directly by the user.

Unlike traditional machine learning and artificial intelligence algorithms, the AXEL A.I. **220** function focuses on the private chain **295** to collect and parse information pertaining to the user and their respective transaction history to enhance the user's engagement and experience within the AXEL blockchain.

In one preferred embodiment, the AXEL A.I. **220** function may collect and parse information pertaining to a video stream viewing history that has been created by the user through their viewing transactions within the AXEL blockchain. The user may query the AXEL A.I. **220** function to obtain the subject history of their stream viewing engagement; along with recommendations for other potential streams the user may be interested in viewing.

The AXEL A.I. **220** function on the private chain **295** is provided and engaged at the sole discretion of the user. The information collected and parsed is stored in the alpha block **210** for recall at the request of the user. The AXEL A.I. **220** information stored in the alpha block **210** is not publicly visible or searchable through the public blockchain **205**. Only the user (not pictured) can access the AXEL A.I. **220** capabilities and the subsequently generated information provided.

On the public chain **205** portion of the AXEL blockchain, the AXEL A.I. **220** function is utilized to promote self-healing within the network. The AXEL A.I. **220** function will collect and parse performance and transaction history from nodes to determine areas of the network that are underperforming or working at a less-than-optimal pace. This information can be collected by the AXEL nodes to aid in isolating problems within the blockchain and creating solutions to ensure the functionality of the AXEL blockchain remains at an optimal level. The AXEL A.I. **220** function on the public chain **205** works in conjunction with the user reputation **225** function discussed below.

The AXEL A.I. **220** function will also utilize a weighting-type algorithm to determine and engage the quickest transactional pathing between nodes participating in the AXEL blockchain. As an example, a transaction may occur within the network that involves multiple nodes for the purpose of transporting the information through the blockchain. The AXEL A.I. **220** function will parse information pertaining to node performance and node reputation to quickly and accurately plot the most direct route for the transportation of information through the blockchain. As more transactions occur, the AXEL A.I. **220** function will continue to monitor, collect, and parse the relevant information on the public chain **205** to ensure self-healing and efficient routing/pathing of transactions and data transportation.

With continued reference to FIG. **2**, the user reputation **225** function gives the AXEL blockchain visibility to positive and negative elements associated with a node and/or a user within the AXEL blockchain.

Reputation information may be collected by the AXEL blockchain relating directly to the functionality of the node or gateway being managed by the user. As stated above, the AXEL A.I. **220** function will collect, parse, and report performance information of the associated network nodes.

In one embodiment, the user node (not pictured) may have introduced incorrect or otherwise non-validated chain data to the AXEL blockchain. The AXEL blockchain would recognize this invalid data through the consensus algorithm (discussed in detail later in this submission) and record the action as a negative for the participating node introducing the invalid data. As the reputation of a user or node moves in a negative direction, the AXEL blockchain may limit or decline participation in one or all activities within the AXEL blockchain. Node and user reputation is paramount to ensuring the security and privacy of the data being exchanged and the users within the AXEL blockchain engaging in these transactions.

If a user or node reputation continues to move in a negative direction, the AXEL blockchain (through the communications and support **275** function discussed later in this submission) will notify the user and/or node to correct the problem. As the user/node performs transactions properly, their reputation may recover. As previously stated, users and/or nodes that continue to receive a negative reputation will be subsequently limited or precluded entirely from activities within the AXEL blockchain.

As with other functional elements within the AXEL blockchain, the user reputation **225** function has both a public chain **205** presence through the alpha block **210**, and a private chain **295** presence. Reputation may be granted in either a positive or negative fashion by the AXEL blockchain as discussed above, but may also be granted in either a positive or negative fashion by a second user or other participant within the AXEL blockchain. As an example, a user may participate in a transaction (through a marketplace element or a file share or transfer) that does not satisfy or meet the criteria of the transaction in a satisfactory manner for the user. The dissatisfied user may grant a negative reputation to the second participant in the transaction to show their displeasure with the subject transaction. The user

may also post a public comment (to a marketplace as an example) where the original transaction took place. As previously stated, when a reputation moves too far in a negative direction the AXEL blockchain may limit or deny the user with a negative reputation from participating in some or all transactional acts until such a time as their reputation has been restored.

The private chain history **230** function serves multiple purposes within the AXEL blockchain. The primary function of the private chain history **230** function is to collect and store transactional information associated with the private chain **295** to ensure that a backup copy exists to support the restoration of the private chain **295** in the case of a failure of a user gateway device that resulted in loss or damage to the private chain **295**.

As transactions occur within the private chain **295**, the history is collected locally through the private chain history **230** function and reported to the public chain **205** for storage in the users' associated alpha block **210**. The private chain history **230** function works in conjunction with the AXEL database **250** function to report and store details of the transactions undertaken by the user.

A second function of the private chain history **230** function is working in conjunction with the AXEL A.I. **220** function to enable a user to parse their history and enable AXEL to provide recommendations for future transactions as described in the examples given previously in this submission. Since the alpha block **210** will always be a component of the network and may not be deleted or removed by any means, the private chain history **230** function, along with other functional **201** elements will be available for recall in case of catastrophic failure on a client device or within the AXEL blockchain.

The AXEL blockchain defines a transaction as any event that creates a block of information that is added to the blockchain. In one embodiment of the AXEL blockchain, a participant may make a purchase utilizing a marketplace being hosted within the AXEL blockchain. This purchase (after being vetted by the consensus algorithm discussed in detail later in this submission) will create a block and add it to the users' private chain **295**. The transaction (block) will be shared **290** with the associated users' alpha block **210** within the public blockchain **205**.

The detailed information collected and stored within the private chain history **230** function is not publicly visible. Only the consensus information is publicly visible. This will ensure that the AXEL blockchain recognizes that all transactions have been authenticated within the blockchain, even though the details of the transactions are not visible. This ensures a level of privacy for the users within the AXEL blockchain while also ensuring the validity of each transaction that occurs.

The AXEL chain communications **235** function (illustrated by reference **290** in FIG. **2**) controls the messaging and data access/movement between the alpha block **210** and the private chain **295**. As an example, the user private chain history **230** function is updated to the alpha block **210** utilizing the AXEL chain communications **235** function and represented by the connection **290** shown between the private chain **295** and the alpha block **210** within the public chain **205**.

The chain communications **235** function occurs constantly within the AXEL blockchain to ensure the information and transactions completed on the private chain **295** are being continuously communicated **290** to the public chain **205** and the subject corresponding alpha block **210**.

The AXEL blockchain incorporates a witness mechanism (discussed in detail later in this submission) that randomly selects a group of five or more network users (or nodes) and utilizes these users to perform the consensus algorithm required to approve a transaction and add a block to the respective private chains of the transaction participants.

The witness administration **240** function governs and manages the aspects associated with creating and managing a witness pool to perform the consensus algorithm. As an example, a user may be selected randomly to perform the consensus algorithm to aid in the resolution of a pending transaction (referred to as the witness mechanism). As the user concludes their consensus session, the resulting verification and the fact that they participated in the subject consensus session will be noted by the witness administration **240** function.

The witness administration **240** function collects and stores (within the AXEL database **250** function) information related to the consensus algorithm function that includes, but is not limited to, the number of times a user and/or node participates as a witness, the number of times the consensus algorithm was executed resulting in a completed consensus, the number of times the consensus algorithm was executed and failed to achieve consensus, and the reputation of the user and/or node as a witness. As explained previously, the user reputation **225** function within the blockchain is vital to ensuring trust and node functionality. The user and/or node reputation relating to the witness administration **240** functions will be stored in both the witness administration **240** and the user reputation **225** functions.

As an example of the above, a user may be randomly selected as a witness by the witness administration **240** function within the AXEL blockchain. Should the consensus be reached successfully and match the consensus of the other participating witnesses, each witness may receive a positive user reputation for reaching a consensus. In a similar fashion, a node that fails to reach the consensus and/or acts in a negative manner pertaining to the network and other nodes may receive a negative user reputation. As previously stated, user reputation is required to remain a participant in good standing within the AXEL blockchain.

The wallet and token administration **245** function controls and manages actions related to both the token(s) that exist within the AXEL blockchain and the wallet mechanism the user and/or node engage to store their token(s). The wallet and token administration **245** function will manage both internal and external wallets that are engaged within the AXEL blockchain. As an example, a user may wish to utilize solely the wallet functionality (not pictured) that exists within the AXEL blockchain. The user may choose to incorporate a second wallet from a 3rd party developer that is used to both store and manage tokens as well as used to purchase and transfer tokens between parties on the AXEL blockchain. The wallet and token administration **245** function will manage each of these wallets according to the configurations set by the user.

As with functions **201** related to the public **205** and private **295** chains within the AXEL blockchain, the wallet and token administration **245** function works in conjunction with other elements including (but not limited to) the AXEL database **250**, the chain communications **235**, the user ID info **255**, the AXEL DCA—Security **285**, the unified device ID info **265**, the Storage/CPU/Mining **280** functions and others. As previously stated transactional information is stored within the alpha block **210** within the public chain **205**.

The AXEL database **250** function engages with other functional **201** elements of the AXEL blockchain to ensure proper routing, tracking, addressing, and historical information is easily available for managing the transactional aspects of the AXEL blockchain. As an example, the AXEL database **250** function may contain routing information associated with user devices (not shown) connected to the AXEL blockchain via the user's personal computer (not shown). The subject routing information makes it possible for the user to access any digital content (e.g. file, folder, etc.) that is managed through or otherwise connected to the AXEL blockchain.

The AXEL database **250** function may also work in conjunction with modules such as the private chain history **230** function to ensure that private chain **295** recovery is possible in case of a catastrophic failure of a client device or other system causing damage to, or deletion of, the user private chain **295**.

The AXEL database **250** function stores AXEL A.I. **220** function information relating to the self-healing aspects of the public chain **205** as discussed earlier in this submission. Weighted routing and pathing information may be stored in the AXEL database **250** function to ensure proper routing of traffic and other transactional aspects that occur between nodes within the AXEL blockchain.

The user ID info **255** function is designated to manage the user engagement with the AXEL blockchain. If configured to work in conjunction with the AXEL DCA—Security **285** function (discussed later in this submission), AXEL can utilize protocol from the Digital Certification Analyzer (U.S. Pat. Nos. 9,419,965; 9,565,184; and 9,723,090) to verify and authenticate the user(s) participating in the AXEL blockchain. The user ID info **255** function collects and manages the user identification, password, pin code, and other pertinent information relating to a user's account. The user ID info **255** function (as stated above) works in conjunction with the AXEL DCA—Security **285** function along with the AXEL database **250** function to store and authenticate user access information.

The user ID info **255** function also works with the unified device ID info **265** function discussed later in this submission to ensure that the login attempts are originating from devices and user(s) that have been verified within the system. As an example, a user may try to log into an AXEL account utilizing a registered device but an incorrect user ID and/or password. The login attempt would subsequently fail. As with the above, a user trying to log into the AXEL account from a non-registered device utilizing an authentic username and password would also fail. The AXEL blockchain requires that both authenticated devices and user accounts are verified through the AXEL DCA—Security **285** function working in conjunction with the AXEL database **250** and the user ID info **255** functions to enable access to a user account within the AXEL blockchain.

The user self-sovereign ID (SSID) **257** controls the detailed identification content of the user such as passport numbers and authentication, driver's license numbers, birth certificates, and other digitally managed identification assets that can be used to positively identify the user. The SSID **257** control creates a block on the private chain **258** that can be utilized by the user/owner of the private blockchain to enable third parties such as vendors, healthcare providers, and others to authenticate the identification of the user.

The SSID **257** will be controlled by a private and public key mechanism that enables the user/owner of the SSID **257** to share a public one-time-use key to any party as a means of accessing the SSID block **258** to confirm the identity of the user. As the authentication of the identification is provided to the third party, that authentication may be captured and stored in an identity vault (not pictured) that is privately stored and backed-up on a user-owned device such as a smartphone, computer, or other digital storage mechanism that can access the AXEL blockchain.

In compliance with emerging privacy laws, future changes thereto, or to adjust to shifting views on data privacy, in some embodiments, an option will exist such that the SSID block **258** can be deleted in whole or in part by the user. It may be desirable that a deletion of a user's SSID block **258** will cause the private chain **295** to immediately back-up some or all transaction content to the alpha block **210** on the public chain **205** and effectively close the account of the user, preventing further engagement with the AXEL blockchain. However, as it is contemplated that the user SSID **257** is utilized solely in instances wherein a transaction requires an extended authentication and validation of the user credentials, the SSID block **258** must remain active in order for the user to participate in such transactions. The AXEL blockchain may be configured such that no user may participate without an SSID block **258**, or that a user without an SSID block **258** may have limited functionality. Common transactions such as certain types of file transfers, including content that is part of the public domain, or a purchase from an online eCommerce site may not require such authorization, and it is contemplated that the blockchain could be configured to allow a user without a complete SSID block **258** to participate in such transactions. Transactions of a significant nature such as the transfer of medical records, the purchase of a property, home, or other physical asset may require the use of the complete user SSID **257** to ensure and authenticate valid user identification.

The network addressing **260** function manages the physical addressing and routing information within the AXEL blockchain. Localized addressing such as communications between the private chain **295** and the respective alpha block **210** is managed through the network addressing **260** function. On a broader scale, the network addressing **260** function ensures that users participating within the AXEL blockchain can efficiently transfer, share, stream, access, store, and otherwise engage with all digital content managed and shared within the AXEL blockchain.

The network addressing **260** function works in conjunction with other functions such as the AXEL database **250** and the AXEL communications **215** (as an example) to enable a first user to establish a messaging and/or chat session with a second user. The network addressing **260** function manages functions associated with directing and routing network traffic on the AXEL blockchain.

The unified device ID info **265** function is utilized to register and authenticate the devices a user uses on the AXEL blockchain. AXEL can incorporate components of the PINApp to enable a user to unify all of the portable computing devices (such as smartphones, tablets, personal computers, and the like) with the AXEL blockchain, providing the capability of accessing any digital content residing on any connected/unified device from anywhere the user or participant travels. This provides the capability of accessing the AXEL blockchain from any device while negating the need to run blockchain gateway software on each device the user engages to access the AXEL blockchain. As an example, a user may be running the AXEL blockchain gateway software on their home PC. The PINApp allows the home PC to communicate directly with the subject user's smartphone, enabling them to access the AXEL blockchain

remotely from their smartphone, negating the need to run a local AXEL gateway client on the subject smartphone.

The unified device ID info **265** function works in conjunction with the AXEL database **250** function to ensure device identification is properly logged and available for access. This function can prevent a user from accessing the AXEL blockchain from an unauthorized device, even if they enter the correct user ID information and associated password(s) and pin codes. As previously stated, privacy, security, and trust between nodes are vital to the functional implementation of the AXEL blockchain. By limiting access to only verified and authenticated users utilizing only authenticated and verified devices, AXEL can guarantee the user within the network is valid. As discussed above, while AXEL may operate with this described security implementation, any variation of security that is desired would be compatible with AXEL. For example, it may be desirable in certain instances to include more or fewer factors of authentication.

The AXEL DCA—Security **285** function works in conjunction with functional elements **201** within the AXEL blockchain. The DCA utilizes a multi-factor algorithm to ensure the positive identity of a user wishing to access the AXEL blockchain, as well as verifying the device in which the user is utilizing to gain access. The unified device ID info **265** function enables the AXEL DCA—Security **285** function to see the physical identity and/or machine code addressing of each device utilized to connect to or otherwise access the AXEL blockchain. If the AXEL DCA is utilized, Security **285** function will only accept an authorized login attempt from an authorized user or participant utilizing an authorized device. It is contemplated that the security setting could be configured in any manner desired. More or fewer authentication factors could be used. Any variation in the login attempt such as a wrong device, wrong username, wrong password, or other incorrect matching with the requirements will be rejected by the AXEL DCA—Security **285** function.

The chain recovery **270** function works in conjunction with the private chain history **230** and the AXEL database **250** functions to restore a user private chain **295** in case of catastrophic failure. In one embodiment, a user may lose access to a gateway device such as a home computer due to a critical device failure. The chain recovery **270** function will enable that user to completely restore their private chain along with the history associated, up to and including the last verified transaction the user participated in.

As stated previously, the public chain **205** is comprised of alpha blocks **210** that may not be completely deleted otherwise removed from the AXEL blockchain. This is due to the fact that transactional information that involves other users may be stored within the alpha block **210**. If it was possible to remove an alpha block **210** it could result in the absence of historical transactional information or witness administration information that could potentially have an impact outside of the first user controlling and managing the subject alpha block **210**, therefore it is impossible to remove an alpha block **210** from the AXEL blockchain.

Should a user wish to delete their account or otherwise end their participation in the AXEL blockchain, their private chain **295** (up to and including the most recent transaction information) may be removed from the AXEL blockchain. However, as previously stated, the private chain **295** information is backed up to the associated public chain **205** alpha block **210** for the specified user. In a preferred embodiment, the chain recovery **270** function allows a user to recreate and/or completely restore their private chain **295**, up to and including the last authenticated transaction executed prior to the private chain **295** removal.

The communications and support **275** function manages system level communications that occur within the AXEL blockchain. This includes, but is not limited to, system level error messages, client/user error messages (in response to errors made by the client/user), technical support queries and responses, alarm and/or alert messages, and the like. In one preferred embodiment, a node may be malfunctioning or generating error codes and introducing them to the AXEL blockchain. The communications and support **275** function may send an error message to the subject node alerting them of the issues and asking them to correct the problem. In another embodiment, a user and/or node may introduce a faulty block into the AXEL blockchain causing the user reputation to diminish. The user and/or node would receive a notification from the AXEL blockchain through the communications and support **275** function, notifying the user and/or node of the subject change in their network standing/reputation.

The communications and support **275** function works in conjunction with multiple functions residing on both the public **205** and private **295** chains including, but not limited to, the AXEL database **250**, the private chain history **230**, witness administration **240**, wallet and token administration **245**, user ID info **255**, network addressing **260**, chain communications **235**, and other functions that engage networking, addressing, and communications functionality within the AXEL blockchain.

The storage/CPU/mining **280** function governs three specific client functions within the AXEL blockchain. The AXEL storage/CPU/mining **280** component of the functional implementation manages the storage repositories of the registered user relating to their own personal storage as well as the storage repositories the user wishes to designate for use in a distributed network storage capability.

The AXEL storage/CPU/mining **280** function enables users to participate in a distributed decentralized network storage capability wherein users (at their total control and discretion) may choose to provide, donate, sell, or otherwise make available for network usage their spare storage space on their node and/or connected devices.

As an example, a user may express the desire to participate in the sale/lease/rental of their spare storage space on a home computer or connected drive through the AXEL blockchain network. The user will notify the AXEL blockchain of their intent to participate and provide information to AXEL as to the amount of storage space they intended to make available, the duration of the space availability, and any limitations they intend to place on the space (if any). The storage/CPU/mining **280** function will collect this information from the user and share it with the AXEL database **250** function. Any second user wishing to engage the storage space can do so through a marketplace or other resource sharing/pooling capability hosted within the AXEL blockchain.

When a user designates drive space as available to the AXEL blockchain, the alpha block **210** will engage multiple AXEL functions **201**, including but not limited to the unified device ID info **265**, the database **250**, the user ID info **255**, the chain communications **235**, the wallet and token administration **245**, the storage/CPU/mining **280** functions and potentially others.

The storage/CPU/mining **280** function provides a CPU pooling function to allow network users to make their CPU available for usage in virtual machine applications. In a similar fashion as shared previously with the network stor-

age example, a user may wish to make their CPU available for virtual machine and/or aggregated computing functionality hosted within AXEL. This capability (as with the distributed decentralized storage described above) is managed through the storage/CPU/mining **280** function.

The virtual machine/aggregated computing functionality (storage/CPU/mining **280** function) enables AXEL to pool the resources of various participating nodes within the blockchain and make that processing power available to users who need more computing power than is currently available to them. Users will be notified by AXEL via the communications and support **275** and/or the AXEL communications **215** functions when their CPU is to be utilized by the AXEL blockchain to process advanced calculations on behalf of other participants in the AXEL blockchain.

As with the storage example provided previously, the storage/CPU/mining **280** function will engage multiple functions **201** within the alpha block **210** including but not limited to the unified device ID info **265**, the AXEL database **250**, the user ID info **255**, the chain communications **235**, the wallet and token administration **245** functions, and potentially others.

As an example, a first user may wish to make available both storage space and CPU processing power through the AXEL blockchain in return for tokens. This sale/rental/leasing configuration may be managed through a marketplace wherein a second user seeking these services may engage the first user selling/leasing/renting these services. In this example, the participants (first and second user) will manage details of their arrangement through the marketplace as they would in any eCommerce setting.

As a transaction is agreed to in the above example, a transfer of tokens would be managed by the wallet and token administration **245** function along with other AXEL functional elements **201** including, but not limited to, AXEL communications **215**, user reputation **225**, chain communications **235**, witness administration **240**, AXEL database **250** functions, and other functional elements **201** within the AXEL blockchain.

The AXEL mining capability managed by the storage/CPU/mining **280** function is the process in which a node participates in resolving a transaction utilizing the consensus algorithm and digitally signs the transaction, creating a new block.

Unlike traditional blockchains that incorporate a mining mechanism, the AXEL blockchain utilizes a mining pool concept (discussed in detail later in this submission) in which each participant in a subject witness (consensus) session will each receive a payment in the form of a utility token (or a relative percentage thereof) for their efforts in executing the consensus algorithm, regardless of whether they are the node that created the actual block or if they were only a participant.

As an example, the witness administration **240** function may select a group of 10 nodes randomly to perform consensus algorithm calculations to verify a subject transaction. Each of the 10 nodes participating in the consensus calculations would receive an identical payment in the form of a token (or a relative percentage thereof) provided they all reached the same consensus during the process. As discussed earlier, nodes failing to reach consensus during a transaction or otherwise introducing incorrect information into the blockchain would receive negative reputation credits for their participation and would therefore be ineligible to receive payment or positive reputation credits.

Mining and transaction consensus activities within the AXEL blockchain are governed by the storage/CPU/mining **280** function (once the witness administration **240** function has created the witness pool). It is important to note, as stated in the example above, a participant continuing to receive negative reputation may be prevented from participating in some or all activities managed through the storage/CPU/mining **280** function as well as other AXEL blockchain transactions.

As stated previously, the alpha block **210** is a component of the AXEL public chain **205**. The purpose of the alpha block **210** is to give the public chain **205** visibility to the elements of the respective user necessary to ensure trust between the nodes and other users, while also ensuring a measure of privacy relating to the transactions of the individual user(s).

In general, alpha blocks **210** are publicly visible **298** but elements within the alpha blocks **210** may not be visible **299**. As an example, each time a block is added to the private chain **295**, the consensus result and digital signature which created the new block is updated **290** to the public chain **205** and the associated alpha block **210**. Detailed information pertaining to the specifics of the transaction such as the name of a file or the file attributes and details may not be visible **299**. Other information such as reputation and some components of the user network ID and addressing are publicly visible **298** as required to enable users to interact with each other and to participate in publicly available functions such as the distributed decentralized storage function, the distributed decentralized CPU (virtual machine) function, and the consensus algorithm (mining) function, and other file storage, sharing, transferring, and communications functions.

For the purpose of ensuring private transactions in a public blockchain environment, many functions **201** hosted within and associated with the alpha block **210** are hidden from public view **299**. These include but are not limited to the AXEL A.I. **220**, the private chain history **230**, the wallet and token administration **245**, the AXEL database **250**, the chain recovery **270** functions, and other functionality that is of a personal and/or private nature.

Should a user or participant cancel their engagement with the AXEL blockchain or otherwise wish to delete their account and their associated transaction history, they may do so except as it relates to the integrity of maintaining historical information in support of other users in the AXEL blockchain. In no case can an alpha block **210** ever be completely removed or deleted from the AXEL blockchain.

As an example, a user may wish to delete their account and cease using the AXEL network. AXEL will remove the user's access to the public alpha block **210** and delete the private chain associated with that user entirely. The alpha block **210** will remain intact and active to ensure that transactions that occurred with the deleted user's participation (such as acting as a witness/executing consensus algorithms, mining, wallet and token exchange functions, and other aspects of functionality that impact other users) remains intact. Deleting an alpha block **210** would result in the activity of the respective user (including group activities such as witnessing transactions and digital signatures) being deleted. This would cause historical references to archived data and past transactions to fail as their references would be eliminated from the blockchain. It is for this reason the alpha blocks **210** may not be completely removed or otherwise deleted from the AXEL blockchain.

Should a user wish to restore their account and engagement with the AXEL blockchain, their original alpha block may be reactivated and their transaction history, up to the time they ceased their engagement with the network, may be restored.

As previously stated the public chain within the AXEL blockchain network works in conjunction with the private (user) chain to manage, track, and store relevant information pertaining to the transaction history and overall user engagement with the AXEL blockchain. The private chain is separated from the public chain to allow AXEL to provide a level of privacy for users enabling private transactions to occur while still maintaining the legitimacy of the consensus algorithm/digital signature component and the subsequent public ledger visibility. The public ledger can remain visible and reflect that the transactions that occurred on the private chain were verified using the consensus algorithm, even though the details of the transactions that occurred on the private chain are hidden from view.

The witness mechanism provided within the AXEL blockchain is a method in which a consensus algorithm may be executed by a group of users (nodes) designated as witnesses for the current transaction being resolved by the blockchain. Witnesses are selected randomly by the AXEL blockchain (utilizing the witness administration function discussed previously with reference to FIG. **2**). In one example, the witness group size may range from 5 users (nodes) up to 20 users (nodes). In the preferred embodiment, the witness group size will be a subset of the nodes not participating in the transaction. It is contemplated that the blockchain could be configured such that the potential witness group size could be any number of users. In one embodiment, the random selection of witnesses to perform each transaction verification (consensus) session takes into account node availability, node/user reputation, and other considerations as discussed above with reference to FIG. **2**.

In a typical blockchain with verifications utilizing a consensus-type algorithm, all nodes participating in the network will work simultaneously to resolve the transaction and create the subsequent block to be added to the subject blockchain. While this consensus mechanism is accurate and gives all nodes (users) visibility to the current transaction being resolved, utilizing all nodes to perform the process limits the thru-put capability of the blockchain and slows the overall rate at which transactions can be verified.

One benefit of the witness mechanism disclosed herein is that it enables multiple transactions to occur and be vetted simultaneously. This will give all users (nodes) visibility to each transaction consensus while speeding up the overall thru-put and transaction speed of the AXEL blockchain.

The witness mechanism utilized to create a group of participants to generate a consensus and create a block for the transactions performed within the AXEL blockchain will now be discussed with reference to FIG. **3**. As previously stated, the typical witness pool may contain between 5 and 20 nodes (users), although the system may be configured for any number that is deemed optimal. The number of nodes (users) performing the witness mechanism with reference to FIG. **3** has been reduced to ease understanding of the witness mechanism.

FIG. **3** represents one possible configuration of the witness mechanism of the AXEL blockchain. The process of the witness engagement begins with a transaction generated by one or more users. As can be seen in FIG. **3**, user **1** as represented by the user private chain **385** engages in a transaction **345** with user **2** as represented by the user **2** private chain **390**. As the transaction is executed between the two users, the user **1** alpha block U**1**A **310** and the user **2** alpha block U**2**A **315** are notified of the pending transaction. The alpha blocks **310** and **315** notify the AXEL public chain **305** through the witness administration function (discussed with reference to FIG. **2**) of the pending transaction **345**. The AXEL public chain **305** executing the witness administration function **381** randomly selects between 5 and 20 users (nodes) to act as witnesses in the pending transaction **345** verification/consensus session to ensure validity of the subject transaction **345** and to create a block on the referenced user chains reflecting the transaction **345**. The AXEL public chain **305** will also incorporate other functional elements of AXEL including, but not limited to, the wallet and token administration **382**, the AXEL database **383**, the network addressing **384**, the unified device ID info **388**, and the storage/CPU/mining **386** functions.

With continued reference to FIG. **3**, the witnesses selected to execute the consensus for the pending subject transaction **345** are witness **1** alpha block **320**, witness **2** alpha block **325**, and witness **3** alpha block **330**. Each of the witness blocks **320**, **325**, and **330** will receive the transaction request and subsequent information from the user **1** alpha block **310** and the user **2** alpha block **315** and begin processing the transaction **345**.

As the transaction consensus session is concluded by the witness pool (witness **1 320**, witness **2 325**, and witness **3 330**) a new block will be created. The user **1** private chain **385** and the user **2** private chain **390** (as private participants in the subject transaction) will each create a block that provides the complete details of the subject transaction **345** and the associated approval therein. On the user **1** private chain **385**, block **335** is added to reflect the transaction **345** that took place with user **2**. On the user **2** private chain **390** a block **340** is created to reflect the details of the subject transaction **345** that took place with user **1**.

As previously noted, the transactions within the AXEL blockchain take place in a private setting. As such, the witness blocks created to reflect the subject transaction **345** will include only the authentication and the digital identification reflecting the transaction but not the details of the transaction **345** that took place between user **1 385** and user **2 390** private chains.

As can be seen in FIG. **3**, the first witness (witness **1 320**) will create a witness block **350** on their private chain **380** to reflect their participation and approval of the subject transaction. In a similar fashion, witness **2 325** will also create a witness block **355** on their private chain **375**, as will witness **3 330** create a witness block **360** on their private chain **370**.

The witness blocks perform multiple functions within the AXEL blockchain. The primary function of the witness block is to provide ledger (chain) verification that the subject transaction took place and was verified. A second function is to ensure that a transaction that has been completed may not be altered, changed, or otherwise removed from the network to ensure multiple copies of the transaction record always exist. Due to the random nature of witness assignment within the AXEL blockchain, bad actors or users wishing to defraud the system will be unable to do so as they will not have visibility to the users (nodes) hosting the witness blocks to reflect the successfully verified and witnessed transactions. Therefore, they will be unable to access and alter, delete, or otherwise compromise the subject transactions.

The witness blocks (**350**, **355**, and **360**) are backed up and stored to their respective user alpha blocks (**320**, **325**, and **330**). This ensures there is always a record of each vetted transaction, even in cases wherein a witness private chain is deleted or a witness otherwise removes their account from the AXEL blockchain.

The user **1** private chain **385** and the user **2** private chain **390** will also update their respective alpha blocks (U**1**A **310** and U**2**A **315**) with the newly added transactions represented

by block **335** on the user **1** private chain **385** and block **340** on the user **2** private chain **390**. Again, these blocks (**335** and **340**) will contain the details of the associated transaction **345** that took place.

In the event that a participant in a given transaction were to delete their account or otherwise remove their private chain from the AXEL blockchain, the transactional information will remain intact in the alpha blocks of the associated user. As shared previously, alpha blocks may not be completely removed or otherwise deleted from the AXEL blockchain to ensure integrity of all transactions that occur.

In conjunction with the witness mechanism as discussed with reference to FIG. **3**, the AXEL blockchain also supports a mining pool capability that enables participants acting as a witness to verify the pending transaction to be compensated for their efforts. Such compensation may be in the form of utility tokens awarded by the AXEL blockchain.

The purpose of the utility token is to allow participants within the AXEL blockchain to engage in transactions that would normally require a method of payment such as a credit card or similar currency mechanism. One benefit of the utility token is that it acts as a substitute for the typically utilized payment mechanisms to allow AXEL to be a completely self-contained system negating the need for an external payment mechanism. As such, participants within the AXEL blockchain can buy, sell, rent and/or lease services and products from each other and utilize the utility token as a form of currency within AXEL.

The mining pool functionality will now be discussed with continued reference to FIG. **3**. As discussed above, the witnesses (represented by private chains **380**, **375**, and **370**) participated in the witness/verification of the subject transaction **345** that occurred between the user **1** private chain **385** and the user **2** private chain **390** (represented by user **1** block **335** and user **2** block **340**).

As the consensus is reached and the mirror blocks **350**, **355**, and **360** are created on the respective witness private chains **380**, **375**, and **370**, the respective witness alpha blocks **320**, **325**, and **330** notify the AXEL public chain **305** of the completed consensus and the subsequent transaction **345**. The AXEL public chain **305** notifies the witness administration **381**, the wallet and token administration **382**, the storage/CPU/mining **386**, and AXEL database **383** functions that the consensus/witness session has successfully concluded. Once the session has been verified by the witness administration **381** function, the witness administration **381** function notifies the wallet and token administration **382** and the storage/CPU/mining **386** functions of the utility token distribution to the respective witness pool. The AXEL public chain **305** will engage the AXEL database **383**, the network addressing **384**, the unified device ID info **388** and the storage/CPU/mining **386** functions to distribute the token reward for processing the subject transaction **345** during the current witness session.

Each witness participant represented in FIG. **3** as witness **1 320**, witness **2 325**, and witness **3 330** will receive a predetermined quantity of tokens or a percentage thereof based on the functional requirements of the blockchain implementation. As an example, each participant may receive one or more tokens for participating as a witness and successfully agreeing on a consensus (resulting in the creation of a new block) in support of the completion of the transaction **345**.

A record of the token award to the above subject witness pool will be logged in each participant's private chain (**380**, **375**, and **370**) along with the AXEL database **383** function.

As discussed previously in this submission, the AXEL blockchain can incorporate elements of the PINApp which is incorporated herein by reference. AXEL can engage the PINApp technology to allow the unification of the storage repositories of client/user connected devices to enable access and management of the content stored on the client/user connected devices through the AXEL blockchain. This unification and connectivity to the AXEL blockchain negates the need for the AXEL blockchain gateway software to be present and functional on each of the client devices, and instead allows aggregation of both the device storage and the device access through a single gateway device. This capability enables a client/user to access, manage, transfer, and stream a file (as an example) that exists on a smartphone to a second user/recipient through the AXEL blockchain without having the subject file physically located on the gateway device. While PINApp provides certain advantages, it is contemplated that other systems with similar capabilities of PINApp could be utilized as well.

The implementation of the PINApp technology with the AXEL blockchain will now be discussed with reference to FIG. **4**. The following discussion on the PINApp implementation will be limited to functional aspects required to support the AXEL blockchain and the associated preferred embodiments.

With reference to FIG. **4**, a personal computer **425** is connected through the PINApp to a tablet computer **405**, an external hard drive **410**, a smartphone **415**, and one or more public cloud services **407**. The personal computer **425** is running the AXEL gateway and is utilizing the AXEL functions **430** to communicate directly with the PINApp functions **455**. As stated previously, the unification as described above makes digital content residing on each of the reference devices available to each other and available to the personal computer **425** running the AXEL gateway. As an example, a file (not pictured) residing on the tablet **405** is available to the personal computer **425**.

The functional elements of AXEL **430** and their engagement with the functional elements of PINApp **455** will now be discussed. The number of functional elements of AXEL **430** and PINApp **455** have been reduced down to provide clarity to the preferred functions.

With continued reference to FIG. **4**, the AXEL communications **432** function works in conjunction with the PINApp **455** functional elements to pass information between the two systems. The AXEL communications **432** function engages with represented PINApp **455** functional elements (user device management **457**, database **460**, file management and control **462**, contact database **465**, cloud server and API management **467**, and addressing and routing **470** functions).

As an example of the engagement between the PINApp **455** and AXEL **430** functional elements, we assume a user (not pictured) who owns the list of devices (personal computer **425**, smartphone **415**, public cloud **407**, tablet **405**, and external hard drive **410**) wishes to share a photograph (not pictured) that resides on smartphone **415** to the AXEL private chain **480** and subsequently the AXEL public chain **475**.

The following example process (with continued reference to FIG. **4**) assumes that both the PINApp **455** and the AXEL **430** functional elements, in conjunction with the personal computer **425** running the AXEL gateway, have verified and authorized the subject user prior to allowing them access to execute the following functional example.

The process begins with the personal computer **425** running the AXEL gateway sending a query from the AXEL

database **440** function through the AXEL communications **432** function to the PINApp database **460** function to identify the photo being shared and the device (smartphone **415**) the subject photo resides on. The PINApp database **460** function (knowing the location of the subject photo residing on the smartphone **415**) will engage the file management and control **462** and the addressing and routing **470** functions to provide the AXEL database **440** function information on the exact location, file name, file address, and other associated data disclosing that the subject file resides on the smartphone **415**.

The AXEL communications **432** function will share the location information with the AXEL database **440**, the AXEL A.I. **435**, the network addressing **442**, and the unified device ID info **445** functions. These functions will enable the AXEL database **440** function to record and verify the location (smartphone **415**) of the subject photo as shared by the referenced PINApp **455** functional modules.

Now that the personal computer **425** running the AXEL gateway has established that the location of the photo is the smartphone **415**, the user (not pictured) may share the subject photo through the private chain **480** and subsequently the public chain **475**. The recipient (not pictured) will access the subject photo directly from the user smartphone **415**, negating the need to relocate, copy, move, or otherwise transfer the photo to a secondary-type repository.

By enabling the PINApp to work directly with the AXEL blockchain users can store, share, stream, and transfer digital content residing on any of their devices through the AXEL blockchain without the requirement to physically move or copy the respective digital content.

In a similar fashion as described above, any digital content residing on any of the devices (tablet **405**, public cloud **407**, external hard drive **410**, smartphone **415**, or even the personal computer **425** hosting the AXEL gateway) may be accessed and managed through the AXEL blockchain by the digital content owner hosting the subject digital content on the above referenced connected (utilizing PINApp) devices.

In another embodiment of the engagement with the functional elements of the PINApp **455** and AXEL **430** it may be assumed that a user controlling the subject connected devices (tablet **405**, public cloud **407**, external hard drive **410**, smartphone **415**, and the personal computer **425** hosting the AXEL gateway) chooses to engage in selling their spare storage space to other users in exchange for utility tokens through the AXEL blockchain. As with the above example, the following example assumes the subject user has already accessed their AXEL blockchain account and has engaged the PINApp and associated security and vetting protocol has been satisfied.

With reference to FIG. **4** the process will begin with the user (not pictured) notifying their referenced alpha block **485** on the AXEL public chain **475** of their desire to participate in the sale of storage resources within the AXEL blockchain. This function will typically occur through an environment such as a marketplace (not pictured) that resides on the AXEL blockchain allowing users to sell extra resources they own and manage for utility tokens.

The marketplace (not pictured) will query the user as to the amount of storage space they wish to make available for sale, the address location of the storage, and the time period or other restrictions the user/seller wishes to place on the sale/lease of the subject storage space.

The user may be accessing the marketplace (not pictured) from any of their reference connected devices, but for the purpose of clarity we will assume the user is utilizing the personal computer **425** hosting the AXEL gateway to configure the storage sale or lease. The user will notify the AXEL blockchain that they wish to make the storage of their external hard drive **410** available for sale or lease to other users within the AXEL blockchain. The AXEL communications **432** function will engage the personal computer **425** and the PINApp **455** functional elements to determine the location and addressing information of the storage space on the external hard drive **410** being put up for sale or lease.

Since the device (external hard drive **410**) is connected to the local user network via the PINApp **455** functions, the AXEL communications **432** function will query the PINApp database **460** function to determine the location of the storage of the external hard drive **410** within the unified network. The PINApp database **460** function, knowing the address location of the external hard drive **410** will engage the user device management **457**, the cloud server and API management **467**, the contact database **465**, and the addressing and routing **470** functions to notify the AXEL functional elements **430** of the location of the associated external hard drive **410**.

Now that the location of the external hard drive **410** is known to the AXEL blockchain, the user (via the personal computer **425** running the AXEL gateway) will provide information to both AXEL **430** and PINApp **455** functional elements pertaining to the user being assigned access to the external hard drive **410** through the AXEL blockchain. Information such as user identification, email address, network address, login, and other access information will be provided to both the AXEL **430** and the PINApp **455** functional elements. The second user (leasing the storage space) access information (identification, email, network addressing, and login) will be added to the AXEL database **440** and to the PINApp database **460** functions. This information will also be available to and managed from the PINApp contact database **465**, the cloud server and API management **467**, the addressing and routing **470**, and file management and control **462** functions under the PINApp **455** functional elements, as well as through the user ID info **437**, the AXEL database **440**, the network addressing **442**, the unified device ID info **445**, the storage/CPU/mining **447**, and the AXEL DCA—Security **450** functions under the AXEL **430** functional elements.

Once the above transactions have been completed, a secondary user (not pictured) may be given access to the subject external hard drive **410** from a remote location from their own devices (not pictured). This secure access will be managed by, and limited to, the provisions as defined under the agreement through the marketplace (not pictured).

Functional elements as described above work in a variety of fashions to ensure the owner of the subject external hard drive **410** and the secondary user utilizing the storage space (not pictured) can maintain their privacy and security while enabling a level of trust to exist between devices since transactions associated with the AXEL blockchain are stored on the private ledger of each participant as discussed earlier in this submission.

As with other distributed and decentralized technologies currently being deployed, the AXEL blockchain does not incorporate a typical client-to-server relationship. The network capability including management of storage and computing resources are provided by users who create nodes to support the network. Therefore, resource management must be handled by the nodes in conjunction with the AXEL blockchain.

The management of network resources such as the availability of user/node provided CPU processing power (sup-

porting the distributed computing function) and the availability of user/node provided storage space (supporting the distributed storage function) within the AXEL blockchain is actively monitored and reported by a resource assessment algorithm.

The resource assessment algorithm routinely queries the AXEL blockchain to determine resource allocation related to both CPU and storage usage as well as to determine the appropriate pathing and trafficking of transactions that occur within the AXEL blockchain.

The resource assessment and traffic pathing capabilities of the AXEL blockchain will now be discussed with reference to FIG. **5**. The diagrams utilized to detail the functional elements of the resource assessment and traffic pathing have been limited to provide clarity of the preferred embodiments. It will be apparent to someone skilled in the art that other capabilities and functional elements exist within the representations and discussions related to the resource assessment and traffic pathing capabilities discussed below with reference to FIG. **5**.

As can be seen in FIG. **5**, the AXEL blockchain **505** is comprised of nodes (**510**, **515**, **520**, **525**, **530**, and **535**) that are owned and managed by users/participants within the AXEL blockchain **505**. A node (**510**, **515**, **520**, **525**, **530**, and **535**) may be a computer or other computing device having one or more processors and one or more storage devices, or access thereto. Node **525** and node **530** are participating in the sale of storage space as reflected by the connected storages **537** (for node **525**) and **539** (for node **530**). This is in support of the decentralized distributed storage capability of the AXEL blockchain **505** as previously discussed.

In one preferred embodiment, the resource assessment algorithm will periodically query the network (each node pictured **510**, **515**, **520**, **525**, **530**, and **535**) to determine the amount of unused (available) storage and compare that with the amount of storage that is currently being used by participants within the AXEL blockchain **505**. The resource assessment algorithm will further run a comparison against storage use history to determine if the currently available storage (unused and available) is satisfactory to support what the algorithm determines as pending needs for the network.

As an example of the above embodiment (and with continued reference to FIG. **5**) the storage/CPU/mining **585** function engages the chain communications **550**, the AXEL database **560**, and the AXEL communications **540** functions to query each of the nodes **510**, **515**, **520**, **525**, **530**, and **535** to determine the currently available amount of storage the AXEL blockchain **505** can support. The feedback from the resource assessment process provides the network addressing **570**, user reputation **545**, and unified device ID info **575** functions to enable AXEL to determine (a) the location of the available storage repositories, (b) the amount of storage available and (c) the address and location information of the provided storage resource(s).

In a situation wherein the network resource (such as storage in this example) is satisfactory to support the network needs as determined by the resource assessment algorithm, no further action will be taken by AXEL. In a situation wherein the network resource is not satisfactory and more resource is needed, one or more nodes (including nodes currently providing storage such as nodes **525** and **530**) will be notified of the need to add storage resources.

Since these nodes are independently operated by users on the AXEL blockchain, they will be invited to participate in supporting network resource needs in exchange for utility tokens (utility tokens) that are used as a form of currency within the network itself. The addition of network resources (such as additional storage space) is entirely at the discretion of the node operator. Should the nodes decide not to add more resources (such as storage) the AXEL blockchain will allow the remaining storage capability to be utilized until such a time as it is at capacity. Once capacity has been reached, the AXEL blockchain will disallow further requests for distributed storage until such a time as resources allow more storage to be provided by the network.

The resource assessment algorithm works in conjunction with other AXEL functional elements **507** to both collect current and relevant statistical information pertaining to the resource availability of the AXEL blockchain **505** as well as to compare and parse this information with historical information to determine the network needs for current and future resource allocation.

As an example (and with continued reference to FIG. **5**) once all of the nodes have been queried by the resource assessment algorithm (as discussed above), the algorithm (controlled by the storage/CPU/mining **585** function) will engage the AXEL database **560** function to collect and parse information relating to historical resource assessment queries to determine network needs.

As discussed earlier, nodes both deploy and control network resources such as storage (as depicted by node **525** with storage **537** and by node **530** with storage **539**) and CPU usage for virtual machine capability (not pictured). Both of these resource needs, along with a variety of others are managed through the resource assessment algorithm function.

Network node-provided resources are governed by not only the resource assessment algorithm, but the user reputation associated with the node(s). As discussed earlier in this submission, node reputation governs the extent at which a node can engage in activities such as providing a witness function, providing decentralized storage for the AXEL blockchain, or providing the CPU capability supporting the distributed computing mechanism (virtual machine capability). As an example (and with continued reference to FIG. **5**) the storage/CPU/mining **585** function will initiate a resource assessment process for the AXEL blockchain **505**. As the assessment begins, the storage/CPU/mining **585** function will query the AXEL database **560** function to collect information pertaining to the AXEL blockchain **505**. The reported information from the database **560** function will include (but is not limited to) the user reputation **545**, the user ID info **565**, the network addressing **570**, the unified device ID info **575** functions, and other associated information to enable the resource assessment algorithm to determine the necessary criteria pertaining to each individual node (**510**, **515**, **520**, **525**, **530**, and **535**). Once the information is collected and parsed by the resource assessment algorithm (controlled by the storage/CPU/mining **585** function), the algorithm will be able to determine (a) the reputation status of each node, (b) the resources available from each node, and (c) any additional qualifying information needed to make the recommendation to support the current or pending needs of the AXEL blockchain **505**.

Assuming all of the nodes within the AXEL blockchain **505** are of an acceptable reputation level (as managed by the user reputation **545** and the AXEL database **560** functions), they will be notified through the chain communications **550** and the communications and support **580** functions of the pending needs of the AXEL blockchain **505** and be invited to participate in providing the required resource. Should a node be disqualified because of a negative reputation (as determined by the user reputation **545** and AXEL database

560 functions) they may be excluded from the network message inviting nodes to participate in providing additional resources. As previously stated, nodes that fall into disfavor within the AXEL blockchain **505** (through negative reputation) will be notified (through the chain communications **550** and the communications and support **580** functions) of their negative reputation and provided guidelines in which the reputation may be repaired. Long-term negative reputation or continued violations may result in the node being removed from participating in network functions, up to and including node deactivation.

As a component of the resource assessment algorithm, the AXEL blockchain **505** provides a mechanism in which transactional traffic can be governed and managed to reduce transaction times while abiding the needs of both the users and the network architecture. Intentionally redundant, the AXEL blockchain **505** (utilizing the resource assessment algorithm) factors into account aspects such as resource allocation, node reputation, node location, ping response times, and other elements to determine how best to manage transactional traffic through the blockchain. This process within the AXEL blockchain **505** is referred to as "weighting" and the above referenced variables determined through the resource allocation algorithm are utilized to determine the proper transaction pathing for a given transaction.

As an example of the weighting process managed through the resource assessment algorithm (and with continued reference to FIG. **5**) a first user represented by node **510** wishes to access remote storage **539** being provided by a second user represented by node **530**. The resource assessment algorithm will first determine if the storage space available at storage **539** via node **530** is suitable for the needs of the first user node **510**. Secondly, the algorithm will determine the reputation of the node **530** to verify that it is within an acceptable level to support the network requirements. Third, the algorithm will send a ping-type signal to test the transaction speeds between the corresponding nodes to determine the fastest route possible for the traffic, while also taking into account the reputation of each node. As the ping-type signal is executed from node **510** it will be sent to node **520**, **515**, and **535**. Assuming all nodes are functioning properly and all nodes are reporting a favorable transaction time and node reputation, the resource assessment algorithm (via the weighting process) will determine the fastest route to engage the storage **539** hosted by node **530**.

Using the above example, we now assume that node **535** has a negative reputation. As the ping-type signal is executed from node **510** it will again be sent to node **515**, **520**, and **535**. Node **535** will report the negative reputation which will require the resource assessment algorithm (weighting process) to either choose the pathing through node **515** or through node **520**. It is important to note that secondary speeds are also considered in determining the most efficient pathing to support transactions.

As an example of the above embodiment, the resource assessment algorithm will seek a complete speed test utilizing the ping-type signal method engaging all nodes and all paths illustrated within FIG. **5**. The shortest path meeting the needs of the AXEL blockchain **505** and the reputation requirements will be chosen.

The AXEL blockchain provides a distributed decentralized CPU processing capability that enables multiple nodes to engage in processing against a user-required program in instances where additional processing power is needed to satisfy the user need. Functioning in a similar fashion to the distributed and decentralized storage capability (discussed below with reference to FIGS. **6** and **7**), the CPU processing capability is a shared resource tool enabling network users to speed processing times of large processing jobs through the utilization of the AXEL blockchain.

The distributed decentralized CPU processing capability follows the same rules as the resource assessment algorithm with reference to traffic, pathing, node engagement, user reputation, and other functional aspects pertaining to the usage of the AXEL blockchain. The distributed decentralized CPU processing capability of the AXEL blockchain will now be discussed with continued reference to FIG. **5**.

A user **501** has a computer processing job **506** that needs to be executed. The processing job **506** is broken down into sections **509** by the AXEL blockchain **505**. These sections **509** are then distributed to the nodes participating in the AXEL blockchain **505** CPU processing capability. As an example, the nodes receiving the sections **509** to be processed may be nodes **510**, **515**, **520**, **525**, and **530**. As the processing job **506** is completed, the resulting sections **509** will be reconstructed by the AXEL blockchain **505** into a single file **506** and returned to the user **501**.

The process is governed by the storage/CPU/mining **585** function and the associated AXEL functions **507** including (but not limited to) the AXEL communications **540**, the user reputation **545**, chain communications **550**, AXEL database **560**, user ID info **565**, network addressing **570**, and the AXEL DCA—Security **590** functions.

The distributed decentralized CPU processing capability (managed through the storage/CPU/mining **585** function) takes into account available resources, user reputations, and transaction times within the AXEL blockchain.

The AXEL blockchain provides a decentralized distributed storage capability that enables users to purchase and sell storage space that is attached to or otherwise managed through their AXEL blockchain connected device(s). In general functional terms, as a user engages the AXEL blockchain storage, digital content (such as a file) may be broken into multiple smaller parts, and then each of the parts may be encrypted to ensure both privacy and security of the stored content as well as to facilitate redundant storage wherein a component or part of a disassembled and encrypted file may reside on multiple storage repositories. The storage mechanism is governed by the AXEL blockchain and deployed and managed by the individual users participating in the sale of storage space within the network.

The decentralized and distributed storage capability will now be discussed with reference to FIG. **6**. While FIG. **6** is limited to show only the primary components and functional aspects of the storage capability, it will become apparent to one skilled in the art that other embodiments exist within the representation.

As can be seen in FIG. **6** a user **605** is connected **635** to the AXEL blockchain **620**. The AXEL blockchain **620** has seven nodes **630**, **640**, **655**, **660**, **670**, **680**, and **690** that are participating in the decentralized and distributed storage capability of the network. The user **605** has a file **610** that they wish to store on the AXEL blockchain **620**. The file **610** is broken down into five separate parts **615**. It is important to note that the number of parts a file will be broken down into varies based on a number of factors including (but not limited to) file size, file type, storage type (i.e. short term, long term, glacial, etc.), and other factors. The file **610** was broken into five parts **615** to ease explanation of the associated storage functionality.

Once the file **610** has been broken down into component parts **615** it is then encrypted. Once encrypted, it is distributed to the AXEL nodes (**630**, **640**, **655**, **660**, **670**, **680**, and **690**) for storage. As can be seen in FIG. **6**, the file compo-

nent parts **615** are stored in a redundant fashion as illustrated by node **630** storing file parts **4** and **5** (**625**) while node **640** is storing the identical file parts **4** and **5** (**645**). The purpose of the redundancy is to ensure that if a node suffers a failure or the file parts should become unavailable for any reason, the AXEL blockchain **620** can enable the user **605** to retrieve them in their entirety. The quantity and location of each file part will vary greatly depending on multiple factors including (but not limited to) the number of nodes in the network that are providing storage, the availability of storage for the user **605** to access, the geographic location of the storage, the transaction speed based on the ping-type signal measurements between nodes, and other factors that govern traffic and user reputation.

Nodes **670**, **680**, and **690** host the identical encrypted file parts (**1**, **2**, and **3**) shown as **675**, **685**, and **695** respectively, while node **660** has stored the entirety of the file parts (**1**, **2**, **3**, **4**, and **5**) as shown **665**. As previously stated, the example referenced in FIG. **6** is a typical configuration of a digital content storage method, but may vary dramatically depending on the variables as described above.

Digital content access, retrieval, and deletion managed through the AXEL blockchain will be administrated through the storage/CPU/mining function (not pictured) that was discussed previously with reference to FIG. **5**. The storage/CPU/mining function will work in conjunction with the resource assessment algorithm (as discussed previously in FIG. **5**) to determine the fastest possible pathing to support digital content access, retrieval, and deletion. Unlike many distributed network architectures, the AXEL blockchain will verify the complete deletion of all digital content parts regardless of location, assuming the storage repository is available and connected to the network at the time of access.

As previously stated, nodes are independently owned and operated by users within the AXEL blockchain. As such, they may choose to remove themselves from service with little or no warning at any given time. The resource assessment algorithm working in conjunction with the storage/CPU/mining function discussed previously will continuously verify the storage repositories and their associated contents to ensure that stored digital content is available to the users who own and manage them. In situations wherein a node is no longer available, the AXEL blockchain (utilizing the resource assessment algorithm in conjunction with the storage/CPU/mining function) will respond to the missing node and recover the missing stored content by copying the missing content (file parts) from a secondary storage point to one or more additional storage points (repositories) to ensure that the content remains available and backed up.

The storage recovery capability will now be discussed with reference to FIG. **7**. As with other discussions and figures provided herein, it is important to note that it will be apparent to one skilled in the art that other functionality exists within the given functional discussion, but has been limited to ease understanding of the preferred embodiments.

As can be seen in FIG. **7** a user **705** has a need to store a file **710**. As discussed previously with reference to FIG. **6**, the file is broken down into parts **715** and encrypted prior to being stored within the AXEL blockchain **720**. The portions of the file (as with previous discussions in FIG. **6**) are stored throughout the network on nodes **730**, **740**, **755**, **760**, **770**, **780**, and **790**.

As can be seen in FIG. **7**, node **790** and subsequent storage **795** has gone offline or has otherwise become unavailable to the AXEL blockchain **720** network. The resource assessment algorithm (managed through the storage/CPU/mining **789** function) has detected the node outage (**790** and storage **795**) and sends a request to the AXEL database **779** function to determine (a) what node and subsequent storage repository has gone offline, (b) what content was stored there and (c) the network address of a working storage repository wherein the missing file parts in storage **795** (1, 2, and 3) can be found. The AXEL database **779** function will provide the requested information, notifying the storage/CPU/mining **789** function that the missing file parts in storage **795** (1, 2, and 3) may also be found at node **780** in storage **785**, node **770** on storage **775**, and on node **760** in storage **765**.

The storage/CPU/mining **789** function will then engage the resource assessment algorithm to query the entire AXEL blockchain **720** network to determine the best location to create additional backup copies of the file parts from storage **795** (**1**, **2**, and **3**) that have gone offline. The resource assessment algorithm (in this example) reported that both node **755** and node **740** were/are suitable to support backup copies of the unavailable file parts from storage **795** (**1**, **2**, and **3**). The storage/CPU/mining **789** function will then copy the missing file parts from storage **795** (**1**, **2**, and **3**) from an existing location (storage **785** from node **780** as an example) and place them into one or more storages as indicated by storage **798** at node **740** and storage **799** at node **755**. The quantity and location of the backup storage repositories (as previously stated) will be determined by the resource assessment algorithm. The algorithm will take into account transaction times and speeds, ping rates between nodes, user reputations, available space, and other attributes to determine the most suitable location for the backup file parts.

As previously discussed, anytime a node is utilized to support storage (such as described above) multiple functional components **759** of the AXEL blockchain **720** may be engaged. These functions can include (but are not limited to) the AXEL communications **749**, user reputation **739**, chain communications **729**, AXEL database **779**, user ID info **719**, network addressing **769**, unified device ID info **709**, communications and support **704**, and the storage/CPU/mining **789** functions.

The AXEL blockchain provides advanced user identification capabilities that allow transactions to occur within the blockchain that would otherwise require face-to-face interaction to ensure identity and transaction verification. Often referred to as AML/KYC (Anti-Money Laundering/Know Your Customer) capabilities, the AXEL blockchain incorporates a user identification mechanism that will allow (when desired based on the nature of the transaction and/or for compliance with laws and regulations) two or more users to participate in a transaction across the blockchain, such as a purchase of an automobile or other high cost item, without the requirement that all parties are in the same place to facilitate the transaction.

The user identification mechanism (AML/KYC function) can be used to support transactions that may require compliance with local, state, federal and/or international laws, as well as ensuring geographical areas under sanction by another governing body can be prevented from participating within the network as governing laws may require or mandate.

In one advantageous embodiment, the user identification (AML/KYC) mechanism utilizes portions of the Digital Certification Analyzer (DCA) U.S. Pat. Nos. 9,419,965; 9,565,184; and 9,723,090 to perform verification of the user and the device being utilized by the user. The user identification mechanism is designed to be implemented in layers within the AXEL blockchain. As an example, a user may be required to only provide an email address and other identi-

fication to participate in the network if they choose not to operate a node or to otherwise not participate in providing functional services to support the network such as the distributed computing/CPU capability or the distributed storage capability. Conversely, a user wishing to provide these types of services through the AXEL blockchain may be subject to further identification and verification such as (but not limited to) passport number, driver's license number, photo ID, or more distinct and descript identification information to ensure that the party's identification can be verified.

The user identification (AML/KYC) mechanism can utilize components of both the PINApp and the DCA to collect and manage information associated with both the user participating in the network as well as the device(s) utilized by the user to engage the network.

The functional aspects of the user identification within the AXEL blockchain will now be discussed with reference to FIG. **8**. As with other discussions provided in this submission, it will become clear to one skilled in the art that other implementations of the stated technology and functionality exist within the discussion. The discussion with reference to FIG. **8** is limited to add clarity to the preferred embodiments. The following discussion assumes the subject user has created an account within the AXEL blockchain and has registered their associated user devices within AXEL.

As can be seen in FIG. **8**, the user local network **801** shows the unification (connection to each other) of each of the user devices: tablet **845**, public cloud storage repositories **850**, smartphone **855**, personal computer **860** running the AXEL gateway software, and an external hard drive **865**. Each of the unified devices have been registered to the AXEL blockchain utilizing the PINApp unification functionality.

PINApp reports the device identification of each of the subject user devices (tablet **845**, public cloud storage repositories **850**, smartphone **855**, personal computer **860** running the AXEL gateway software, and an external hard drive **865**) to the AXEL database **815** function. This information is stored within the AXEL database **815** function in conjunction with the user account creation and login information.

As an example of the functional elements during a login session wherein the user is seeking to gain access to the AXEL blockchain, we assume the user is logging into their account through the tablet **845**. The user will enter their login criteria and submit it to the AXEL DCA—Security **840** function. The AXEL DCA—Security **840** function will engage the AXEL database **815** function to authenticate information including (but not limited to) the user login information, the tablet **845** unified device ID info **830**, the network address **825** of the tablet **845**, the user ID info **820**, and potentially other functional elements to verify (a) the user credentials and (b) the device authorization. Should a user provide a valid user identification and an invalid device authorization, the login attempt will fail. Conversely, if the user identification is invalid but the device is authorized, the login attempt would again fail.

The AXEL DCA—Security **840** function will be engaged each time a user seeks to access the AXEL blockchain or any associated device, even after they have achieved a login session. As an example, we assume the user has logged into the tablet **845** as stated above. The user then wishes to access content stored on their external hard drive **865** that is unified with other client devices (tablet **845**, public cloud storage repositories **850**, smartphone **855**, and personal computer **860** running the AXEL gateway software). As the user access request is initiated, the AXEL DCA—Security **840** function will access the AXEL database **815** function to collect the unified device ID info **830**, the user ID info **820**, and the network addressing **825** to ensure that the user (via tablet **845**) is authorized to access the external hard drive **865**.

As previously stated, the AXEL DCA—Security **840** function will verify multiple data points including (but not limited to) user identification info **820**, network addressing **825**, and unified device ID info **830** along with a PIN and TOKEN mechanism that is a component of the DCA to ensure the user is authorized to access the information stored on the subject external hard drive **865**.

The above process will repeat through the system anytime a user wishes to engage any of the unified local network (**801**) devices that comprise their registered device network utilized within the AXEL blockchain.

In instances where a user local network **801** is providing storage (such as the external hard drive **865**) for sale or usage by the AXEL blockchain, the AXEL DCA—Security **840** function will verify (utilizing the process above) both the user/owner of the storage device as well as any user(s) registered within the AXEL blockchain who is given permission to access the storage. The verification for the user(s) accessing the storage will include a check of permissions as set by the user/owner of the storage and hosted within the AXEL database **815** function. As stated previously, these permissions will be set at the time the distributed storage capability is offered publicly for use by the user/owner of the storage device.

The user verification process described above operates continuously throughout the AXEL blockchain at any time a user wishes to engage any device registered within the network. This prevents a user from logging into a network-accessible account on a registered device and then subsequently switching out that device for one that is not registered to the network.

What is claimed is:

1. A system for verifying and maintaining privacy of one or more transaction records between users with a public ledger, the system comprising:

a plurality of node devices comprising one or more processors and one or more storage devices;

a public ledger stored on one or more storage devices of the plurality of node devices, wherein the public ledger comprises a plurality of blocks;

a plurality of private ledgers associated with one or more of the plurality of blocks of the public ledger; and

a witness pool comprising a subset of the plurality of node devices wherein said witness pool is used to witness a transaction between at least two node devices and verify one or more transaction records, wherein the subset of the plurality of node devices does not include the at least two node devices;

wherein the witness pool generates one or more mirror blocks for each of the one or more transaction records with the one or more processors, and adds the one or more mirror blocks to the plurality of private ledgers, wherein one or more of the plurality of blocks is updated to include a verification of the one or more transactions;

wherein the one or more mirror blocks include details from the one or more transaction records while the plurality of blocks do not; and

wherein the details from the one or more transaction records included in the one or more mirror blocks remain private.

2. The system of claim 1, wherein the witness pool is assigned a utility token upon verification of the one or more transaction records.

3. The system of claim 1, wherein the subset of the plurality of node devices in the witness pool are randomly selected.

4. The system of claim 1, wherein the one or more transaction records are selected from the group consisting of storage space, processing time, and data purchase records.

5. The system of claim 1, wherein the plurality of private ledgers are stored on the one or more storage devices of the subset of the plurality of node devices in the witness pool.

6. The system of claim 1, wherein the one or more mirror blocks are encrypted.

7. The system of claim 1, wherein one or more of the plurality of node devices execute a gateway application that causes communication of at least a portion of the public ledger to one or more client devices via the one or more of the plurality of node devices.

8. A system for verifying and maintaining privacy of one or more transaction records between users with a public ledger, the system comprising:

a plurality of node devices comprising one or more processors and one or more storage devices;

a public ledger stored on one or more storage devices of the plurality of node devices, wherein the public ledger comprises a plurality of blocks;

a plurality of private ledgers associated with one or more of the plurality of blocks of the public ledger; and

a witness pool comprising a subset of the plurality of node devices wherein said witness pool is used to witness a transaction between at least two node devices and verify one or more transaction records, wherein the subset of the plurality of node devices does not include the at least two node devices;

wherein one or more of the plurality of blocks is updated to include a verification of the one or more transactions;

wherein information is added to at least one private ledger concerning the transaction; and

wherein the private ledger includes at least some information concerning the transaction that remains private and is not available on the public ledger.

9. The system of claim 8, wherein the information added to at least one private ledger concerning the transaction is added to a private ledger associated with a node that participated in the transaction.

10. The system of claim 8, wherein the information added to at least one private ledger concerning the transaction is added to a private ledger associated with a node that was part of the witness pool for the transaction.

11. The system of claim 8, wherein a node in the witness pool is provided compensation for participation in a witness pool.

12. The system of claim 8, wherein witness pool is assigned a utility token upon verification of the one or more transaction records.

13. The system of claim 8, wherein a node must have an associated private ledger in order to participate in a transaction.

14. A computer-implemented method for verifying and maintaining privacy of one or more transaction records between at least two node devices with a public ledger and a plurality of node devices, the plurality of node devices comprising one or more processors and one or more storage devices, the method comprising:

storing the public ledger on the one or more storage devices of the plurality of node devices, wherein the public ledger comprising a plurality of blocks;

associating one or more private ledgers with one or more of the plurality of blocks of the public ledger;

generating one or more mirror blocks for each of the one or more transaction records with a witness pool comprising a subset of the plurality of node devices, wherein the one or more mirror blocks are generated by the one or more processors of the subset of the plurality of node devices in the witness pool and the subset of the plurality of node devices does not include the at least two node devices;

adding the one or more mirror blocks to the one or more private ledgers, wherein the one or more of the plurality of blocks associated therewith are updated to include a verification of the one or more transactions; and

storing the one or more private ledgers on the one or more storage devices of the subset of the plurality of node devices in the witness pool;

wherein details from the one or more transactions in the one or more mirror blocks remain private.

15. The computer-implemented method of claim 14, wherein the one or more private ledgers include details from the one or more transaction records while the plurality of blocks do not.

16. The computer-implemented method of claim 14 further comprising assigning a utility token to the witness pool upon verification of the one or more transaction records.

17. The computer-implemented method of claim 14, wherein the subset of the plurality of node devices in the witness pool are randomly selected.

18. The computer-implemented method of claim 14, wherein the one or more transaction records are selected from the group consisting of storage space, processing time, and data purchase records.

19. The computer-implemented method of claim 14 further comprising encrypting the one or more mirror blocks.

20. The computer-implemented method of claim 14 further comprising executing a gateway application on one or more of the plurality of node devices that causes communication of at least a portion of the public ledger to one or more client devices via the one or more of the plurality of node devices.

* * * * *